Identification And Review Of The Department's Major Information Technology Systems Inventory

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 07-37
June 2007

IDENTIFICATION AND REVIEW OF THE DEPARTMENT'S MAJOR INFORMATION TECHNOLOGY SYSTEMS INVENTORY

EXECUTIVE SUMMARY

This audit report responds to a directive contained in the fiscal year (FY) 2006 Department of Justice appropriations bill conference report that the Office of the Inspector General (OIG), among other things, provide an inventory of major Department of Justice (DOJ) information technology (IT) systems.[1] In a prior report, the OIG developed a preliminary inventory of DOJ IT investments based on DOJ's reporting to the Office of Management and Budget (OMB). In this report, the OIG has refined the inventory to identify 38 major DOJ IT systems and to provide cost and other information on the 38 systems. In addition, this OIG audit provides information on the way that DOJ collects cost information for its IT investments.

In this report, we provide information on DOJ's IT inventory, including system names, descriptions, DOJ component owner, future funding requirements, and implementation status. This information is discussed throughout the report and is summarized in the report appendices.

We also attempted to provide cost data on each of the DOJ's major systems. Because DOJ's financial systems do not provide sufficiently detailed cost data on individual IT systems, we collected cost information from DOJ components' IT system managers.

This report includes cost data provided by the components for the 38 major DOJ systems. In addition, we attempted to perform detailed testing on the costs of three IT systems from the components responsible for the majority of DOJ's IT spending – the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), and Justice Management Division (JMD) – to verify the accuracy of the cost information.

We found that the DOJ's approach to IT system cost reporting is fragmented and lacks the management controls necessary to ensure the accuracy and completeness of system cost data. Moreover, our detailed testing of the costs of the three sampled systems confirms

[1] Conference Report for the Fiscal Year 2006 Science, State, Justice, Commerce, and Related Agencies Appropriations Act (P.L. 109-108).

that DOJ does not have complete cost data for any of these IT systems. We determined that the $327.9 million combined costs reported for these three systems was understated by at least $68 million.

We also found that the methods DOJ components use to track and report the actual costs of IT systems vary. Even within DOJ components, such as the FBI, differences in methods also exist for collecting cost information for different IT systems. We found that IT system managers are generally responsible for developing and maintaining the cost data they report, and neither the Chief Information Officers (CIO) at the component and DOJ levels nor the Department Investment Review Board (DIRB) evaluates and approves the methods used or test the validity of the cost data reported.[2]

Although our audit did not examine the components' core financial systems in detail, we found that the cost data contained in these systems generally does not allow a determination of individual IT system costs.

Background

Since FY 2001, Congress has authorized more than $12 billion for DOJ IT equipment, software, and services – an average of over $2 billion annually. In FY 2007, DOJ spending authority represents approximately 4 percent of the $64 billion authorized for IT across the federal government and approximately 11 percent of DOJ's annual budget.

DOJ IT decision-making and oversight involves Congress, OMB, the DIRB, and CIOs at the DOJ and component levels. DOJ and component CIOs are required to manage their respective Capital Planning and Investment Control processes in accordance with the Clinger-Cohen Act of 1996 and OMB directives.[3] The Clinger-Cohen Act defines Capital Planning and Investment Control (CPIC) as the process for maximizing the value, and assessing and managing the

[2] The DIRB is a group chaired by the Deputy Attorney General and vice-chaired by the DOJ CIO that is responsible for Department-level oversight of major DOJ IT investments and for ensuring that components' IT investments are aligned with DOJ's IT strategy. The DIRB also includes senior DOJ officials with IT and financial management expertise.

[3] The Clinger-Cohen Act is codified in 40 U.S.C. § 11312 (1996).

risks, of executive agency IT acquisitions. As part of this audit, we reviewed documents that contain DOJ IT system cost data, including OMB Exhibits 300 (Business Case) and OMB Exhibit 53 (IT Investment Portfolio).

Congressional Request

The conference report for P.L. 109-108 directs the OIG to: (1) produce an inventory of all major DOJ IT systems and planned initiatives, and (2) report on the effectiveness of DOJ's IT planning efforts. In a prior report, the OIG developed a preliminary inventory of investments based on DOJ's reporting to OMB, which we have refined for this report to identify major DOJ IT systems.[4]

In this report, we provide a more detailed inventory that includes the following information for each major DOJ IT system:

- system name
- system description
- DOJ component owner
- cost
- implementation status

In addition to reporting on the inventory of major DOJ IT systems, the OIG was asked to provide another report detailing all research, plans, studies, and evaluations that DOJ has produced, or is in the process of producing, concerning its IT systems, needs, plans, and initiatives. A separate OIG audit report will present this analysis.

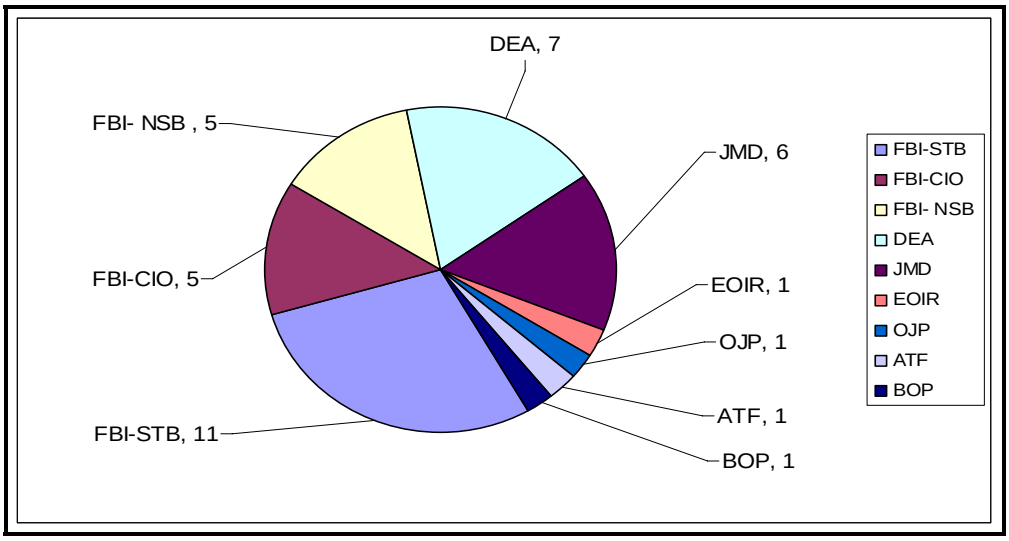
[4] Department of Justice, Office of the Inspector General. *Inventory of Major Department of Justice Information Technology Investments as of FY 2006*, Audit Report Number 06-25, March 2006.

Inventory of DOJ IT Systems and Projects

In developing an inventory of major DOJ systems, we identified 38 major IT systems operated by, or under development in, 7 DOJ components. The FBI has the largest number of IT systems in the inventory with 21, followed by the DEA with 7, and JMD with 6.[5] Because these three components make up nearly 90 percent of the total inventory, we focused on these three components' IT cost-reporting practices in this audit.

The following chart shows the distribution of all 38 major DOJ IT systems and projects by component, with a further breakout by major FBI entity.

Distribution of IT Inventory



Source: OIG

The following table lists the 38 major IT systems in DOJ's IT inventory, grouped by DOJ component.

[5] Although the Organized Crime Drug Enforcement (OCDETF) Fusion Center is located within the Office of the Deputy Attorney General, for purposes of this audit we included the Fusion Center IT system as part of the DEA. The DEA's unobligated funds developed the Fusion Center.

DOJ Inventory of 38 IT Systems and Projects by Component

Component	Systems and Projects
FBI	**21 Systems and Projects**
FBI STB	**Science and Technology Branch – 11 Systems and Projects**
1	Integrated Automated Fingerprint Identification System
2	Next Generation Integrated Automated Fingerprint Identification System
3	National Instant Criminal Background Check System
4	National Crime Information Center
5	Law Enforcement Online Re-engineering/Relocate
6	Law Enforcement National Data Exchange Rev 9/7
7	Combined DNA Index System
8	Electronic Surveillance Data Management System
9	Digital Collection
10	Biometric Reciprocal Identification Gateway/Criminal Justice Information Sharing Interoperability Initiative
11	Computer Assisted Response Team Storage Area Network
FBI OCIO	**Chief Information Officer Branch – 5 Systems and Projects**
1	Sentinel
2	Data Centers
3	Technical Refresh Program
4	Investigative Data Warehouse
5	Multi-Agency Information Sharing Initiative Regional Data Exchange
FBI NSB & Security Div	**National Security Branch and Security Division – 5 Systems and Projects**
1	Terrorist Screening Center
2	Foreign Terrorist Tracking Task Force
3	Security Management Information System
4	Information Assurance Technology Infusion
5	Sensitive Compartmented Information Operational Network
DEA	**7 Systems and Projects**
1	Model 204 Corporate Systems
2	E-Commerce-Controlled Substances Ordering System
3	EPIC Information Systems
4	Concorde
5	FIREBIRD
6	Merlin
7	OCDETF Fusion Center System

JMD	6 Systems and Projects
1	Integrated Wireless Network
2	Unified Financial Management System
3	Litigation Case Management System
4	Classified Information Technology Program
5	Justice Consolidated Office Network
6	Public Key Infrastructure
ATF	National Integrated Ballistics Information Network
BOP	Inmate Telephone System-II
EOIR	eWorld
OJP	Grants Management System

Source: OIG analysis

Cost Data for DOJ's Major IT Systems

One of our objectives was to determine the actual amounts DOJ has spent on the 38 IT systems identified in the inventory. To accomplish this, we first considered using data from the core financial systems used by the various DOJ components and their related IT systems. However, we found that the components' financial systems are not required to organize data for CPIC cost reporting purposes and thus do not contain costs for individual IT systems.

We next considered any control procedures specific to reporting IT system costs. However, none of the three components whose individual system we tested in depth – the FBI, DEA, or JMD – had established control procedures to ensure that the actual costs reported for their IT systems were complete and accurate. We concluded that component CIOs lack the control procedures necessary to ensure accuracy and completeness in the CPIC cost reporting function and this likely contributed to incomplete costs reported for the DOJ IT systems we tested.

Because we lacked a source of cost data for individual IT systems within the DOJ, the OIG developed a questionnaire related to the 38 major systems in the inventory. Through the DOJ CIO, we distributed these questionnaires to the components' IT system managers. The completed questionnaires included: (1) annual costs incurred since the system's inception through FY 2005, (2) estimated funding requirements through FY 2012, and (3) a description of the cost tracking methods used by each IT system.

The following table shows the total costs of the 38 major DOJ IT systems through FY 2005 and the amounts estimated through FY 2012, as reported to us by the components' system managers.

Costs Incurred and Estimated as Reported for the 38 Major DOJ IT Systems

Component	Actual Costs Incurred through FY 2005[a]	Actual and Estimated Costs through FY 2012
FBI – 21 systems	$ 3,344,267,750	$ 8,629,480,672
DEA – 7 systems	$ 1,176,437,903	$ 2,276,009,456
JMD – 6 systems	$ 984,461,302	$ 3,771,279,876
ATF, BOP, EOIR, and OJP - 1 system each	$ 222,596,693	$ 394,855,788
Total DOJ	$ 5,727,763,649	$ 15,071,625,792

Source: OIG analysis of completed questionnaires

[a] Due to rounding, values do not sum.

Testing the Accuracy of Reported Costs

Next, we judgmentally selected 3 of the 38 questionnaires completed by the IT system managers in the 3 components with the most IT systems – the FBI, DEA, and JMD – to perform tests on the accuracy of the cost data for "Actual Costs Incurred through FY 2005."

Due to the insufficient internal controls over the completeness of the costs reported, we assessed as "high" the risk that DOJ IT system costs may be understated. Accordingly, we focused our attention on determining whether the costs reported for the IT systems were complete.

Testing for the completeness of costs without a means of sampling transactions from the entire financial system is considerably more difficult than simply confirming that reported costs exist. Although we used components' financial and budget system data to the extent possible in attempting to verify the costs reported to us, we cannot provide assurance that our audit has identified all the costs associated with the three selected IT systems.

The systems we selected for testing are:

- FBI's Law Enforcement Online (LEO),
- DEA's Concorde, and
- JMD's Justice Consolidated Office Network (JCON).

The following table shows the costs each system manager provided us through FY 2005 and the cost amounts identified by the OIG for each of these systems.

Comparison of Components' Reported Costs and Costs Identified by the OIG for Three Sampled Systems
($ in millions)

IT System Tested	Amount Reported by Component	Amount Identified by OIG	Amount of Difference[a]	Percentage Difference
LEO	$ 115	$ 128	$ 13	11%
Concorde	$ 19.8	$ 21.3	$ 1.5	8%
JCON	$ 194	$ 246	$ 53	27%

Source: OIG analysis

[a] Due to rounding, not all values sum.

In the next sections, we describe our results for each of these three systems.

Law Enforcement Online

LEO is the FBI's Internet-based communication system and information service for law enforcement agencies nationwide. Thousands of police officers and other employees of local, state, and federal law enforcement agencies are able to access LEO 24 hours a day, 7 days a week.

In its completed questionnaire, the FBI reported $115 million in total costs incurred for LEO through FY 2005. The two largest elements included $74 million related to a cooperative agreement with Louisiana State University (LSU) that developed the LEO system and $30 million for FBI salaries and benefits to maintain the system.

To test the completeness of the reported amounts associated with the FBI's cooperative agreement with LSU, we obtained a listing of all payments the FBI made to LSU from the FBI financial system. Reconciling all the financial system payment information and the reported amounts would have taken an inordinate amount of time, but from a random review of some of the FBI financial system's listed payments, we identified five requisitions related to LEO totaling $850,000 that were not included in the project management cost data. We also obtained directly from LSU amounts invoiced to the FBI since 1995 when LEO was created. When we compared the LSU and FBI amounts for LEO, the LSU amounts were more than $13 million greater than the amounts recorded by the FBI.

FBI officials told us it was likely the LEO cost data was missing LSU transactions from all FBI divisions. Because LEO's costs are tracked by the FBI Criminal Justice Information System (CJIS) Division, LEO activity involving other divisions or offices of the FBI must be reported to the CJIS to be included in the LEO cost reports.

Finally, we verified that approximately 30 FBI employees are working on LEO-related activities, and we concluded that the reported costs averaging $3 million annually over the 10-year period are reasonable.

Concorde

Concorde is a DEA system designed to integrate DEA's IT functions, improve business processes, and enable information sharing within the DEA. It is intended to allow DEA Special Agents, Intelligence Analysts, and other investigative professionals to manage investigative case files digitally. The central feature of the Concorde system is the Investigative Management Program and Case Tracking System (IMPACT), a web-based case management system.

In responding to our request for Concorde cost information, the DEA reported that the project began in 2000, with related costs through FY 2005 totaling $19.8 million. The DEA's response to our questionnaire also stated government personnel costs amounted to $3.7 million, and that five contractors were individually paid at least $1.3 million over this same period.

The DEA's financial system is not organized to easily and reliably identify all the costs associated with any particular IT system. However, in FY 2005 DEA finance staff created a unique code for

Concorde funding. This code was established so the financial system could easily track funding specifically allocated for Concorde. DEA finance staff provided us with a financial system report that captured all activity associated with the Concorde funding code in FYs 2005 and 2006. To the extent possible, we tested the completeness of contract costs contained in this financial system report for FYs 2005 and 2006.

By comparing the financial system report to the Concorde project management cost data, we identified $702,555 in omitted software expenditures. DEA officials told us the incomplete project management cost data may have been related to the accounting treatment for Concorde's software expenditures, which requires these costs to be reported as an asset in DEA's financial statement throughout the development phase rather than as an expense. In addition, we determined that expenditures totaling approximately $770,000 during the first 2 years of the project were not included in DEA's response to our request.

We also evaluated the $3.7 million in government personnel costs DEA reported for Concorde, or approximately $600,000 annually between FYs 2000 and 2005. Although our analysis suggests that these costs are reasonable, these amounts are not based on actual data. DEA officials told us they have no procedures for tracking the time its employees spend working on any particular project, and the personnel costs are estimates made at the beginning of the fiscal year.

Justice Consolidated Office Network

JCON is the common office automation platform administered by JMD that over 70,000 employees from 16 DOJ components use daily. JCON provides IT tools and services that allow these employees to perform their computer-based work duties.[6] Specifically, JCON provides the basic IT computing framework for DOJ, which includes hardware such as networked workstations and printers, and applications such as e-mail and word processing. JCON also provides the infrastructure for components to access other IT systems, such as case management databases and DOJ's Financial Management Information System.

The JCON system manager reported $193.6 million in total costs since FY 2001, including $50 million paid to BAE Systems, the single

[6] The amounts discussed below represent JCON Planning and Acquisition only. JCON maintenance is funded by the 16 participating DOJ components.

largest contractor that provides full life cycle support services for JCON. From an overall listing of payments DOJ made to this contractor – containing over 1,400 payments totaling more than $149 million – we identified 504 payments related to JCON made between FYs 2002 and 2005 totaling $49,537,777. The difference between the value we calculated and the value reported by JCON is $89,135 – less than 1 percent of the reported costs.

We also discussed financial issues with the JCON Project Management Office (PMO) and learned it would be possible to create a report from the financial system that could identify planning and acquisition-related costs to JCON. The PMO provided us with a report that matched the $193.6 million figure reported to us on our questionnaire. Officials told us this amount included the government full-time equivalent (FTE) costs incurred over the period.

In addition to comparing FY 2005 CPIC and budget data, we compared the $246 million total amount reported to OMB in the JCON Exhibit 300 for planning and acquisition to the $193.6 million total amount reported in the OIG questionnaire. JCON officials told us that total costs in the Exhibit 300 were $53 million more than total costs reported to the OIG because the Exhibit 300 includes expenditures from FYs 2000 and 2001 and are not considered part of the current version of JCON, which is called JCON IIA.

We researched government and industry sources for more information on JCON and JCON contracts. This search identified a $500 million JCON contract awarded in 1996, more than 5 years before the first costs reported in our questionnaire. Although the PMO response to our questionnaire made clear that the reported costs relate to JCON IIA, we consider the JCON initiative to have begun in 1996 when the decision was made to replace disparate office automation systems with a consolidated system.

The JCON PMO confirmed that this first attempt at replacing existing office automation systems, known as JCON I, began in 1996 and was ultimately terminated along with the contract in 1998 when it did not work. JCON II followed JCON I and evolved into JCON IIA by FY 2002. Because the earlier JCON efforts predate the current JCON Project Manager and other staff, they were not able to provide us with the complete costs for JCON prior to FY 2002.

In summary, by using financial system and budget data we were able to verify the costs the JCON Project Management Office reported

to us. However, the Project Management Office said these costs only represent the current standard architecture, JCON IIA, and not previous versions of JCON. Although JMD views the various versions of JCON as separate systems, we believe the true cost of JCON should include all costs incurred since 1996 when the JCON project was initiated. Therefore, we conclude that JCON's costs since 1996 should be at least $53 million more than the $193.6 million we verified. In addition, because complete cost data was not available for JCON prior to FY 2002, we were unable to determine what amounts, if any, were paid in connection with the 1996 $500 million contract.

Conclusions

We found that IT system cost reporting within the DOJ is fragmented and lacks the management control procedures necessary to ensure such cost tracking is accurate and complete.

Moreover, DOJ does not have complete cost data for the three IT systems we tested and, based on our testing and review of data produced by DOJ's financial and budgeting systems, in general we lack confidence in the accuracy of the cost data reported for DOJ's IT systems. In our opinion, the lack of complete cost data that is verifiable for DOJ's IT systems compromises the effectiveness of DOJ's IT oversight entities, including Congress, the OMB, the DIRB, and DOJ and component CIOs.

In this report, we make three recommendations to improve the accuracy and completeness of DOJ's reporting of IT system costs. The recommendations involve: (1) ensuring that components develop methods of reporting of actual and verifiable IT system costs, (2) better integrating OMB Exhibits 53 with budget submissions, and (3) assessing the feasibility of using the planned Unified Financial Management System for consistent and accurate reporting of individual IT system costs.

TABLE OF CONTENTS

INTRODUCTION

The conference report for the fiscal year (FY) 2006 Science, State, Justice, Commerce, and Related Agencies Appropriations Act (P.L. 109-108) directs the Office of the Inspector General (OIG) to: (1) produce an inventory of the Department of Justice's (DOJ) major information technology (IT) systems and planned initiatives, and (2) report on the effectiveness of DOJ's IT planning efforts. This audit report responds to the congressional request to compile an inventory of DOJ's major IT systems.

In this report, we provide the following information for each major system:

- system name
- system description
- DOJ component owner
- cost
- implementation status

Audit Methodology

The OIG developed a three-phase approach to respond to the congressional request. In the first phase of this effort, we used DOJ's IT Investment Portfolio – known as the Office of Management and Budget (OMB) Exhibit 53 – to preliminarily identify the universe of major IT and other investments.[7] In March 2006, we issued the Phase I report that listed unaudited information on 46 IT investments listed in the OMB Exhibit 53.[8]

In Phase II, we attempted to verify the DOJ's IT system inventory and the information requested in the conference report. This report provides the results of that review.

In Phase III, the OIG will provide a separate report detailing all research, plans, and studies and evaluations the Department has produced concerning IT systems, needs, plans, and initiatives. The

[7] The OMB Exhibit 53 IT investments report include systems, projects, offices, salaries, and other IT related costs.

[8] Department of Justice, Office of Inspector General. *Inventory Of Major Department Of Justice Information System Investments as of Fiscal Year 2006*, Audit Report Number 06-25, March 2006.

OIG's Phase III report also will identify the depth and scope of any problems DOJ has experienced in the formulation of its IT plans.

Identifying the Inventory of Major IT Systems and Projects

Our Phase I report identified 46 major DOJ investments with appropriations of $15 million and higher between FYs 2005 and 2007.[9]

In this report, we refined this universe of investments by applying criteria for defining major IT systems. By reviewing those entities with oversight of DOJ IT spending and the projects or systems they currently are monitoring or have an interest in, we identified the inventory of 38 major IT systems and projects.

The following table lists the entities with oversight responsibilities for DOJ's IT spending and actions that indicated to us a particular IT system or project is major.

[9] The Exhibit 53 that DOJ provides to OMB combines all its systems related to office automation and infrastructure and reports them in a single entry called Consolidated Enterprise Infrastructure. Although our Phase I report did not cite the individual IT systems that comprise the Consolidated Enterprise Infrastructure, we have done so in this report.

DOJ IT Spending Oversight Entities and Functions

IT Spending Oversight Entity	Actions Indicating an IT System or Project is Major
Congressional Appropriations Committees	IT system is mentioned in the Conference Report to the Appropriations Bill.
Office of Management and Budget	OMB requests a business case (Exhibit 300) for an IT system or project, or selected for compliance with Earned Value Management requirements.[a]
Department Investment Review Board (DIRB)	An IT system or project that is monitored by the DIRB.
Office of the Chief Information Officer (OCIO)	A system or project is monitored in the OCIO's Dashboard.[b]

Source: OIG

[a] Earned Value Management is a tool that measures the performance of a project by comparing the variance between established cost, schedule, and performance baselines and what is actually taking place.

[b] The Dashboard IT project monitoring tool is described in the Findings section of this report.

The roles of these oversight entities and the methods they employ to monitor major IT systems or projects follow.

DOJ's IT Spending Oversight Structure

DOJ's IT oversight structure is based primarily on provisions contained in the Clinger-Cohen Act, 40 U.S.C. § 11312 (1996). At the time the Clinger-Cohen Act was passed, Congress recognized that the federal government had failed to modernize its information technology systems, resulting in billions of wasted taxpayer dollars.

The major provisions of the Clinger-Cohen Act increased the authority and responsibility of officials at OMB and other Executive Branch agencies, including DOJ, in the following ways:

- The OMB Director is required to promote and improve the acquisition, use, and disposal of IT by the federal government to improve the productivity, efficiency, and effectiveness of federal programs.

- The Attorney General is required to design and implement a process for maximizing the value, and assessing and managing the risks, of IT acquisitions.[10]

- The DOJ Chief Information Officer (CIO) is required to provide advice and other assistance to senior management to ensure IT is acquired and managed in a way that promotes the effective and efficient design and operation of all major information resources.[11]

In addition to the structure established by the Clinger-Cohen Act, Congress directed the DOJ to establish the DIRB, led by the Deputy Attorney General, which we describe below.

Another feature of the IT spending oversight structure at the DOJ is the restriction on reprogramming or making use of funding for purposes beyond those established in the annual appropriation process. As with other types of spending, DOJ is required to notify the Appropriations Committees in both the Senate and House 15 days in advance of any reprogramming that exceeds the limitations established in the law.

DOJ IT Spending Oversight Entities

Four primary entities oversee DOJ's IT spending: (1) the congressional appropriations committees, (2) OMB, (3) the DIRB, and (4) DOJ's OCIO. By identifying the IT systems these four oversight entities are currently monitoring, we refined our universe of major IT systems. In the remainder of this report, we provide cost and other information related to 38 major IT systems.

Congressional Appropriations Committees. The Appropriations Committees and Subcommittees of the Senate and House of Representatives are responsible for reviewing the President's Budget, receiving testimony from government officials, and appropriating funds for the federal government. In recent years, these committees have expressed concern over DOJ's high-profile IT system failures, such as the Federal Bureau of Investigation's (FBI) Virtual Case File case

[10] The Clinger-Cohen Act defines this process as an agency's Capital Planning and Investment Control process.

[11] In addition to a CIO for DOJ, the Clinger-Cohen Act anticipated that a CIO would be established as needed at DOJ components.

management system, as well as the large amount of resources devoted to IT. Consequently, 13 IT systems cited in the Conference Report to the FY 2006 Science, State, Justice, Commerce, and Related Agencies Appropriations Act are included in our revised inventory of major IT systems.[12]

Office of Management and Budget. OMB is responsible for assisting the President in overseeing the preparation of the federal budget and supervising its administration. With regard to IT spending at Executive Branch agencies, each fiscal year OMB reviews the business cases, presented on OMB Exhibits 300, for a number of IT systems and projects. The Exhibit 300 includes information on individual IT system program and procurement planning, risk mitigation and management planning, realistic cost and schedule goals, and measurable performance benefits. The Exhibit 300 also includes a summary of prior years' spending.

Our list of major IT systems includes 18 of 19 IT systems and projects for which OMB requested DOJ to submit Exhibits 300 in the FY 2006 budget cycle.[13]

Related to OMB's evaluation of agency Exhibits 300 is OMB's Management Watchlist. OMB maintains this list to identify those projects needing improvement in performance measures, Earned Value Management, or system security. At the time we finalized this report in March 2007, there were no DOJ IT systems on the OMB Management Watchlist.

In addition to monitoring IT capital plans using the Exhibits 300, OMB has established requirements for the use of Earned Value Management tools for certain DOJ IT systems and projects. These requirements are designed to improve execution and performance of all new major IT projects, ongoing major developmental projects, and high-risk projects. DOJ's OCIO staff provided us with a list of the 16 IT systems and projects with Earned Value Management tools that have already been validated or are to be validated.[14] All of these IT

[12] For this list of IT systems and projects, see Appendix II, Table A.

[13] The OIG did not include the Exhibit 300 for the FBI's Special Technologies and Applications Section (STAS) because it is an FBI subdivision that included numerous IT projects and systems. For this list of IT systems and projects, see Appendix II, Table B.

[14] For this list of IT systems and projects, see Appendix II, Table C.

systems and projects are included in our inventory of major DOJ IT systems.

OMB also maintains a list of high-risk IT systems that require additional monitoring. This list is developed with the participation of the agencies according to criteria that OMB established in an August 2005 memorandum. This memorandum required agencies to identify IT systems as high risk if the system meets one or more of the following criteria:

- The agency has not consistently demonstrated the ability to manage complex projects.
- There are exceptionally high development, operating, or maintenance costs, either in absolute terms or as a percentage of the agency's total IT portfolio.
- The project is being undertaken to correct recognized deficiencies in the adequate performance of and essential mission program or function of the agency, a component of the agency, or another organization.
- Delay or failure would introduce for the first time unacceptable or inadequate performance or failure of an essential mission function of the agency, a component of the agency, or another organization.

Eight of the nine DOJ IT projects on the OMB high-risk list are included on our inventory of major DOJ IT systems.[15] We excluded one project – grants.gov because of its relatively small dollar amount.[16]

Department Investment Review Board (DIRB). The DIRB is a group chaired by the Deputy Attorney General and vice-chaired by the DOJ CIO. The DIRB also includes senior DOJ officials with IT and financial management expertise. The stated purpose of the DIRB is to provide DOJ-level oversight of major IT investments and ensure component investments are aligned with DOJ's IT strategy. One of the

[15] For this list of IT systems and projects, see Appendix II, Table D.

[16] Grants.gov is an interagency system managed by the Department of Health and Human Services for on-line grant applications and grant fund management through a common website.

DIRB's main functions is to hold the IT managers accountable for their projects and ensure "return on investment" considerations are paramount in governance decision-making.[17] According to its charter, the DIRB selects for oversight between 5 and 12 investments for review in any year, and this oversight may continue for the life of the project at the discretion of the Board Chair and Vice Chair. We met with the DOJ Chief Systems' Architect who is a member of the DIRB, and obtained a list of 11 systems and projects the DIRB is monitoring. All 11 of these systems and projects are included in our inventory of major DOJ IT systems.[18] However, the DIRB does not evaluate or approve the methods used to determine, or test the validity of, the cost data reported to it by the IT system managers.

Office of the Chief Information Officer (OCIO). The OCIO is required to develop and maintain DOJ's IT strategy and establish an IT architecture. The OCIO also is responsible for ensuring that the activities of the components comply with DOJ's strategy and architecture. One of the management tools the OCIO uses to monitor IT systems and projects is the OCIO Dashboard. The Dashboard provides – on a monthly basis – the DOJ CIO, component CIOs, and project managers with current status information on major and other highly visible IT systems in DOJ's IT Investment Portfolio. The Dashboard attempts to track cost, schedule, performance, risk, and other major issues for IT systems. Currently the OCIO is tracking 33 IT systems and projects with the Dashboard. Twenty-two of these 33 Dashboard projects and systems are included in our inventory of major DOJ IT systems.[19]

[17] "Return on investment" in this context means the quantitative benefits that will be achieved through an investment in the IT system. Examples of these benefits are systems' savings, cost avoidance, and stakeholder benefits.

[18] For this list of IT systems and projects, see Appendix II, Table E.

[19] In order to focus our review on the largest systems, we included those systems with a cumulative cost of $15 million and higher for FYs 2005 through 2007. We also included four IT systems monitored by the OCIO Dashboard that do not have 3-year costs exceeding $15 million because they met additional criteria. For this list of IT projects and systems, see Appendix II, Table F.

FINDINGS AND RECOMMENDATIONS

The OIG identified 38 major DOJ IT systems and collected cost and other information on these systems from DOJ components. DOJ components reported $5.7 billion in incurred costs for these systems through FY 2005 and estimated total costs of $15 billion through FY 2012. We determined that DOJ has fragmented and inconsistent systems and methodologies for reporting IT system costs and lacks the controls necessary to ensure accuracy and completeness. Also, DOJ's financial systems are not designed to provide cost data on an individual IT-system basis and were therefore not useful as a source of cost data.

We believe the lack of complete cost data that is verifiable for DOJ's IT systems compromises the effectiveness of DOJ's IT oversight entities, including Congress, OMB, the DIRB, and DOJ and component CIOs.

Our audit work also included detailed testing of costs reported for a sample of the three IT systems in the FBI, DEA, and JMD – the three components responsible for the majority of DOJ's IT spending. We determined that the $327.9 million in combined costs reported for these three systems was understated by at least $68 million.

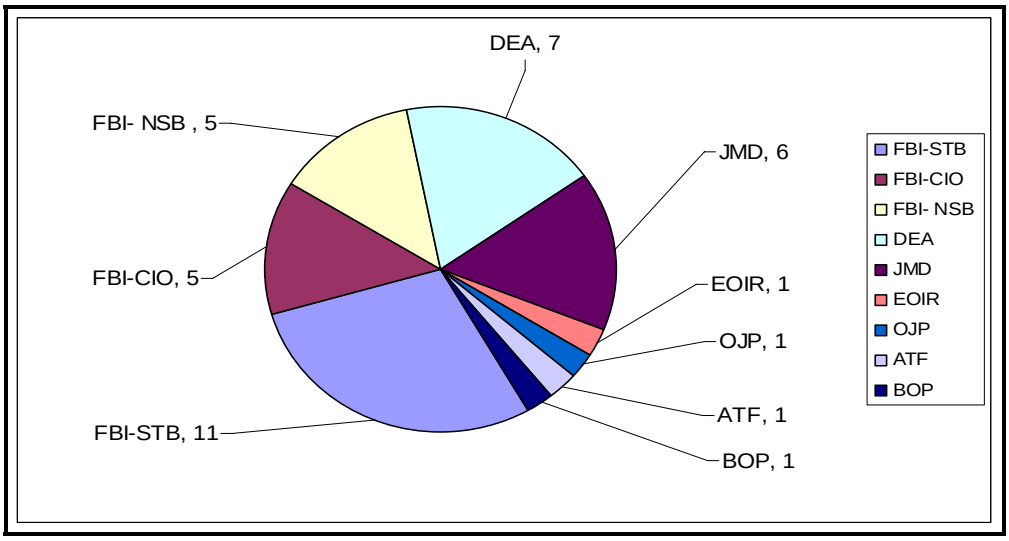
Inventory of Major DOJ IT Systems and Related Costs

We identified 38 IT systems operated by, or under development in, 7 DOJ components as the inventory of major DOJ systems. The FBI has the largest number of IT systems in the inventory with 21 – clustered in the OCIO, Science and Technology Branch (STB), and National Security Branch (NSB) and Security Division. The DEA has seven systems on the list and JMD has six.[20] Because these three components make up nearly 90 percent of the total inventory, we focused on their IT cost reporting practices in this audit.

The following chart shows the distribution of all 38 major DOJ IT systems and projects.

[20] Although the Organized Crime Drug Enforcement (OCDETF) Fusion Center is located within the Office of the Deputy Attorney General, for purposes of this audit we included the Fusion Center IT system as part of the DEA. The DEA's unobligated funds developed the Fusion Center.

Distribution of IT Inventory



Source: OIG

After an initial survey that included interviewing Department and component IT and finance staff, we determined no component-level or DOJ-wide systems collect data on individual IT system costs. To obtain the best available data on the 38 major IT systems in the inventory, we asked the managers of each system to provide us with detailed cost and other information on the systems they manage. System managers reported $5.7 billion in system costs through FY 2005 and an additional $9.3 billion estimated through FY 2012, for a total of $15 billion.

The IT systems managers completed an OIG-developed questionnaire, distributed through the DOJ CIO, that requested costs and timeframes associated with each phase of the project's system development life cycle, total costs incurred through FY 2005, funding amounts and funding sources necessary to complete the system, contractor information, a brief description of the methods used to determine reported costs, and other information required to respond to the congressional request.

Based on the responses to our questionnaire and additional interviews of component IT staff, we confirmed that IT system cost reporting across the Department is fragmented and inconsistent. The methodologies used to track the costs of IT systems vary widely among and within components, and there is a general lack of controls necessary to ensure accuracy and completeness.

The primary objective of the OIG questionnaire was to obtain comparable cost data on all 38 major IT systems. The following table shows the detailed cost and the estimated funding required for the inventory of 38 major DOJ IT systems.

IT System Costs Reported on OIG Questionnaire

	System	To Date Costs through 9/30/2005	Funding Requests – FY 2012	Total Costs through FY 2012
FBI - Science and Technology Branch				
1	Integrated Automated Fingerprint Identification System	$ 1,515,162,000	$ 812,008,000	$ 2,327,170,000
2	Next Generation Integrated Automated Fingerprint Identification System	$ 14,094,000	$ 438,726,000	$ 452,820,000
3	National Instant Criminal Background Check System	$ 393,684,000	$ 408,706,000	$ 802,390,000
4	National Crime Information Center	$ 315,404,000	$ 162,276,000	$ 477,680,000
5	Law Enforcement Online Re-engineering/Relocate	$ 114,536,000	$ 237,989,000	$ 352,525,000
6	Law Enforcement National Data Exchange Rev 9/7	$ 25,235,000	$ 195,242,000	$ 220,477,000
7	Combined DNA Index System	$ 4,780,000	$ 92,759,000	$ 97,539,000
8	Digital Collection	$ 200,150,000	$ 205,530,000	$ 405,680,000
9	Electronic Surveillance Data Management System	$ 25,454,195	$ 148,120,000	$ 173,574,195
10	Biometric Reciprocal Identification Gateway /CJIS Interoperability Initiative	$ -	$ 346,662,000	$ 346,662,000
11	Computer Assisted Response Team Storage Area Network	$ 16,328,000	$ 92,859,000	$ 109,187,000
FBI - OCIO Branch				
12	Sentinel	$ 4,300,000	$ 433,667,000	$ 437,967,000
13	Data Centers	$ 450,000,000	$ 200,895,322	$ 650,895,322
14	Technical Refresh Program	$ 24,400,000	$ 380,400,000	$ 404,800,000
15	Investigative Data Warehouse	$ 84,436,523	$ 135,065,296	$ 219,501,819
16	Multi-Agency Information Sharing Initiative Regional Data Exchange	$ 7,957,843	$ 10,000,000	$ 17,957,843

FBI - National Security Branch and Security Division				
17	Terrorist Screening Center	$ 22,030,000	$ 453,676,000	$ 475,706,000
18	Foreign Terrorist Tracking Task Force	$ 82,046,000	$ 142,900,000	$ 224,946,000
19	Security Management Information System	$ 3,633,190	$ 76,993,000	$ 80,626,190
20	Information Assurance Technology Infusion	$ 2,554,379	$ 5,300,000	$ 7,854,379
21	Sensitive Compartmented Information Operational Network	$ 38,082,620	$ 305,439,304	$ 343,521,924
DEA				
22	Model 204 Corporate Systems	$ 334,556,000	$ 96,159,860	$ 430,715,860
23	E-Commerce-Controlled Substances Ordering System	$ 24,315,070	$ 79,310,032	$ 103,625,102
24	EPIC Information Systems	$ 63,821,000	$ 71,830,108	$ 135,651,108
25	Concorde	$ 19,784,000	$ 50,813,000	$ 70,597,000
26	Firebird	$ 639,533,346	$ 551,397,000	$ 1,190,930,346
27	Merlin	$ 90,904,000	$ 109,730,144	$ 200,634,144
28	Organized Crime & Drug Enforcement Task Force Fusion Center System	$ 3,524,487	$ 140,331,409	$ 143,855,896
JMD				
29	Integrated Wireless Network	$ 752,302,000	$ 1,818,096,000	$ 2,570,398,000
30	Unified Financial Management System	$ 25,580,973	$ 403,062,668	$ 428,643,641
31	Litigation Case Management System	$ 3,500,000	$ 99,563,360	$ 103,063,360
32	Classified Information Technology Program	$ -	$ 38,118,003	$ 38,118,003
33	Justice Consolidated Office Network	$ 193,567,064	$ 270,078,542	$ 463,645,606
34	Public Key Infrastructure	$ 9,511,265	$ 157,900,000	$ 167,411,265
ATF				
35	National Integrated Ballistics Information Network	$ 125,000,000	$ 122,000,000	$ 247,000,000
BOP				
36	Inmate Telephone System-II	$ 361,693	$ 205,095	$ 566,788
EOIR				
37	eWorld	$ 19,482,000	$ 26,352,000	$ 45,834,000
OJP				
38	Grants Management System	$ 77,753,000	$ 23,702,000	$ 101,455,000
Totals[a]		**$5,727,763,649**	**$9,343,862,143**	**$15,071,625,792**

Source: OIG analysis of completed questionnaires

[a] Due to rounding, values do not sum.

After obtaining and analyzing the data provided by the individual system managers, we attempted to verify costs associated with one IT system from each of the three DOJ components (FBI, DEA, and JMD), which collectively represent over 97 percent of all the IT spending in our audit inventory.

In the following sections of this report, we briefly discuss our consideration of the Department's IT Capital Planning and Investment Control environment, budget, and financial systems in order to complete our verification of the Department's major IT inventory.

IT Capital Planning and Investment Control Environment

Since FY 2001, Congress has authorized more than $12 billion for DOJ IT equipment, software, and services – an average of more than $2 billion annually.[21] DOJ spending authority represents approximately 4 percent of the $64 billion authorized on IT across the federal government in FY 2007 and 11 percent of DOJ's annual budget.[22] These funds are used to acquire new computers and other assets as well as to cover expenses associated with operating and maintaining legacy IT systems. Funding for new acquisitions and improvements to existing IT is referred to as Development, Modernization, and Enhancement (DME) costs, while operating expenses are known as "steady state" costs. In FY 2005, DOJ spending authority related to steady state activities amounting to nearly $1.5 billion – more than double the $702 million allocated to DME expenditures.

More than 40 DOJ components or organizational units use IT systems to assist DOJ's 104,000 employees in the performance of their duties and to provide support for the state and local law enforcement community.

In addition to the DOJ CIO, each major component has a CIO.[23] Each of these components has either its own Capital Planning and Investment Control (CPIC) policies and IT investment management (ITIM) processes, or follows DOJ's policies and processes. In prior audit reports, the OIG reviewed the ITIM processes at three DOJ

[21] DOJ IT spending authority for FY 2006 is an enacted amount.

[22] The DOJ's FY 2006 enacted budget is approximately $22 billion.

[23] The DOJ CIO is organizationally located in JMD and serves as CIO for both the DOJ and the JMD component.

components – the FBI, DEA, and JMD – and found they are in the beginning or middle stages of their ITIM processes.[24]

Although the DOJ and component CIOs have important roles and input to decision-making on IT matters, they often do not control the budgets for the IT systems they are responsible for monitoring. DOJ officials could not estimate what percentage of DOJ spending is controlled by offices other than the OCIO, because each component budgets its IT spending differently.

Elements of an agency's CPIC process include IT planning, establishing an IT architecture, and monitoring the status of IT systems. Although the DOJ CIO and component CIOs we reviewed have significant responsibilities for their organization's IT systems, we found they also have varying degrees of control over those IT system budgets.

The Clinger-Cohen Act outlines the required content of an agency's CPIC process:

- provide for the selection of information technology investments to be made by the executive agency, the management of such investments, and the evaluation of the results of such investments;

- be integrated with the processes for making budget, financial, and program management decisions within the executive agency;

- include minimum criteria to be applied in considering whether to undertake a particular investment in information systems, including criteria related to the quantitatively expressed projected net, risk-adjusted return on investment and specific quantitative and qualitative criteria for comparing and prioritizing alternative information systems investment projects;

- provide for identifying information systems investments that would result in shared benefits or costs for other federal agencies or state or local governments;

[24] See Appendix III for information on prior reports examining the DOJ's ITIM process.

- provide for identifying for a proposed investment, quantifiable measurements for determining the net benefits and risks of the investment; and

- provide the means for senior management personnel of the executive agency to obtain timely information regarding the progress of an investment in an information system, including a system of milestones for measuring progress, on an independently verifiable basis, in terms of cost, capability of the system to meet specified requirements, timeliness, and quality.

Because we had difficulty obtaining independently verifiable cost data for the major IT systems in the inventory, we discussed with DOJ OCIO staff whether the DOJ and its components are complying with the Clinger-Cohen Act provision cited above.

OCIO officials told us that to meet the Clinger-Cohen Act requirements, they are now using Earned Value Management tools for IT investments under development. Because OMB has only recently required Earned Value Management for new IT investments, historical cost data for these systems would not have been available to use for this audit. Therefore, the Clinger-Cohen Act provisions would be met only for new systems under development.

The IT Investment Portfolio

A report known as the IT Investment Portfolio or Exhibit 53, required by the Clinger-Cohen Act and the Paperwork Reduction Act of 1995, is designed to help OMB and other federal agencies provide a full and accurate accounting of an agency's IT investments. The Exhibit 53 is a product of the IT CPIC and ITIM processes. As the name suggests, the CPIC process should enable an agency to plan, acquire, and manage its IT acquisitions. During the CPIC process, the agency CIO is responsible for collecting and managing the data necessary for the preparation of the IT Investment Portfolio.

The IT Investment Portfolio is similar to the President's Budget in that each item in the IT Exhibit 53, whether a system, project, or service, is reported with 3 years of associated spending. The 3 years used in the Exhibit 53 are the budget year, the current year, and the prior year. The spending reported for all years reflects the appropriated amounts or budgetary resources available for that year.

The costs of individual IT systems are usually included in the programs and activities of a component with other costs, including those of other IT systems. These other costs are called object classifications, or object classes.[25] DOJ component CIOs do not generally compile the actual cost data they report in the IT Investment Portfolio because they rely on individual IT system managers to collect and report cost data that the CIOs review before it is submitted to OMB.

To inform Congress of IT spending, OMB provides Congress with an Exhibit 53 at the time it submits the President's Budget. Both DOJ's budget and Exhibit 53 include IT spending but use different formats to present the same appropriations – actual, enacted, and proposed. Both of these documents may appear to be integrated, but they are created for different purposes by separate offices and use different databases to gather information.

To collect and process most of the information needed to prepare DOJ's budget, OMB uses the MAX budget system.[26] DOJ enters its budget and financial data into the MAX system, which organizes the data using a series of schedules, including the object classification schedule.

[25] Object classification is spending based on an item or service purchased by the federal government. In this case, object classes break down total IT system costs into smaller costs such as personnel compensation, equipment, and advisory or assistance services.

[26] The MAX Budget Information System is used to support the federal budget process. OMB uses the MAX Budget Information System to collect, validate, analyze, model, and publish budget information.

The following table from Circular A-11 shows how various IT obligations should be assigned to object classes:

MAX Budget System Object Classes for IT Spending

Description of Obligation	Object Class Number	Object Class Title
IT services or rental of IT equipment	23.3	Communications, utilities, and miscellaneous charges
Operation and maintenance of IT systems by the private sector	25.7	Operation and maintenance of equipment
Operation and maintenance of IT systems by another Federal Government Account	25.3	Purchases of goods and services from Government Accounts
IT hardware and software	31.0	Equipment
IT supplies and material such as manuals, diskettes, and toner cartridge	26.0	Supplies and materials
IT consulting for management, studies, analyses, and evaluations, or engineering and technical services	25.1	Advisory and assistance services

Source: OMB MAX

In addition to the instruction on how to assign different types of IT obligations to object classes, OMB directs agencies to include employee wages in the personnel compensation and benefits object class even when these employees are working to develop an IT system.[27]

While the MAX budget system is used for the President's Budget, OMB uses the Electronic Capital Planning and Investment Control (eCPIC) system, which is installed on agency intranets, to collect IT Investment Portfolio data. The eCPIC system is designed to manage and control IT spending and help prepare information requested by OMB. In addition to facilitating the preparation of the IT Investment Portfolio, the eCPIC system also contains the data used to prepare Exhibits 300 for individual IT systems.

[27] OMB Circular A-11 states that the object classes present obligations according to their initial purpose, not the end product or service. For example, for a federal employee who constructs a building, the obligations for the employee's wages should be classified under personnel compensation and benefits rather than acquisition of assets.

The following table summarizes the differences between DOJ-related sections of the President's Budget and the IT Investment Portfolio.

Comparison of the President's Budget to the IT Investment Portfolio

Cost Report	President's Budget	IT Investment Portfolio
Scope	All Spending	IT Spending Only
DOJ amounts in FY 2005	$28 billion	$2 billion
OMB system to collect data	MAX	eCPIC
Related agency process	Budget Execution	Capital Planning and Investment Control
Related responsible agency officer	Chief Financial Officer	Chief Information Officer
Related agency staff preparing cost data	Chief Financial Officer's Budget and Finance Staff	Individual IT system owners
Related agency systems	Core Financial Systems capturing all agency transactions - audited	Various ad hoc methods and cost databases - no one system capturing all agency transactions - not audited

Source: OMB and DOJ documents

DOJ Core Financial Systems

Core financial systems are used for the funds management function of an agency. These systems should ensure that agency financial transactions are captured and processed in a uniform and consistent manner.

Data from DOJ components' core financial systems is put in a format that defines all costs of individual IT systems. Without the ability to identify and extract data in a useable format, it is cumbersome and time consuming to identify the costs of these IT systems. Therefore, auditing the costs of the 38 major IT systems in

DOJ's inventory would, in essence, require a detailed audit of each system.

In this review, we focused on the core financial systems maintained by the FBI, DEA, and JMD. The FBI's core financial system, Federal Management System (FMS), is a legacy system dating back to the 1980s. In general, FMS limits the FBI's ability to process financial information effectively and efficiently, including timely financial statements.

At the start of our audit, we discussed with FBI officials familiar with FMS the possibility of extracting and summarizing cost data in FMS for the individual IT systems in the inventory. These officials told us that financial data in FMS is not coded in sufficient detail to allow this kind of independent identification and grouping for all IT systems.

We also met with DEA and JMD officials to determine whether their respective financial systems – the Federal Financial System (FFS) and Financial Management Information System (FMIS) – could be used to identify or verify costs of individual IT systems. Although the FFS and FMIS are newer systems and do not have the same degree of limitations as the FBI's FMS, neither system can easily produce reports that identify all the costs associated with its components' IT systems.

Despite the age and weaknesses of these financial systems, officials told us this financial data could have been more useful had accounts been created and transactions consistently coded to track IT systems as defined in the CPIC process. This did not occur because the primary cost tracking concern of the components is related to the overall budget and spending process rather than the CPIC process. Additionally, cost reporting for CPIC purposes is not specifically required by law for federal financial systems.[28]

[28] The Office of Federal Financial Management's *Core Financial System Requirements* issued in January 2006 requires the following seven functions: financial system management, general ledger management, funds management, payment management, receivable management, cost management, and reporting.

Verification of IT System Cost Data

We selected three IT systems within the FBI, DEA, and JMD, – LEO, Concorde, and JCON, respectively – based on the results of the OIG-developed questionnaire. Within those three systems, we tested the accuracy and completeness of the actual cost data reported. Due to the lack of sufficient internal controls or any routine testing of the accuracy of the costs reported, we assessed the risk as "high" that all IT system costs may be understated. Accordingly, we planned our work and focused on determining whether the costs reported by the IT systems were complete. Testing for completeness without the ability to sample transactions from the entire financial system is considerably more difficult than simply confirming the reported costs exist. Although we used component financial and budget system data to the extent possible, there is no assurance that our work has identified all the costs associated with these three IT systems.

FBI Law Enforcement Online

Law Enforcement Online (LEO), which was formed through a cooperative agreement between the FBI and Louisiana State University (LSU), is the FBI's Internet-based communication system and information service for law enforcement agencies nationwide. Thousands of police officers and other employees of local, state, and federal law enforcement agencies are able to access LEO 24 hours a day, 7 days a week.

Examples of the services available to users of LEO include:

- E-mail – Provides the capability to send and receive messages electronically between LEO users.

- Topical Electronic Library – Provides an easily accessed repository of law enforcement publications, studies, research, and technical bulletins.

- Distance Learning – Provides online topical learning modules that can be used at any time of day or night at the user's own pace with instructional feedback.

In response to our questionnaire, the FBI Criminal Justice Information Services (CJIS) Financial Management Unit provided the cost information.[29]

LEO Costs
($ in millions)

FY Start	Costs incurred through FY 05	Estimated Funding through FY 2012	Total Costs Through FY 2012
-- [a]	$ 115	$ 238	$ 353

Source: OIG analysis of completed LEO questionnaire

[a] The FBI did not provide a LEO start date on its completed questionnaire.

Although the LEO response did not indicate a start date, FBI and LSU documents indicated the system was created in 1995 and transferred from a FBI unit to CJIS in 1997.

We met with CJIS Financial Management Unit officials to discuss the source of the amounts reported in our questionnaire and their methods for tracking actual costs. These officials told us the $115 million in costs through FY 2005 comprised personnel and non-personnel costs, but no indirect costs. In addition, non-personnel costs included costs associated with a cooperative agreement with LSU. The following table presents the breakdown of actual LEO costs through FY 2005.

LEO Reported Costs for FYs 1995-2005
($ in millions)

Non-personnel		
Cooperative Agreement with LSU	$ 52	
Other	$ 33	
Total non-personnel		$ 85
Total personnel		$ 30
Total costs		**$ 115**

Source: CJIS documents

[29] Established in 1992, CJIS serves as the focal point and central repository of criminal justice information services at the FBI.

LEO's direct, non-personnel requisitions are tracked in the CJIS Budgetary and Evaluation and Reporting System (BEARS) database.[30] However, the CJIS Financial Management Unit does not use BEARS to report LEO's costs for CPIC purposes. Instead, officials use electronic spreadsheets primarily for budget monitoring. CJIS Financial Management Unit officials provided us with copies of these electronic spreadsheets and demonstrated how they sorted the data to calculate the direct, non-personnel amount included on our questionnaire. This amount, $85 million, comprises 74 percent of the total LEO costs reported through FY 2005.

Not all of the LEO-related expenditures reported were incurred by CJIS, since LEO was under different management until 1997. Since that time, other FBI divisions have participated with funding and managing LEO activities.

At the time CJIS Financial Management Unit officials provided us the LEO cost spreadsheets, they identified an error in their original response. As a result, the amount related to LSU was increased from $52 million to $74 million. However, this restatement did not change the overall reported costs of $115 million or the percent of direct, non-personnel costs described above.

To test the completeness of the reported LEO costs, we compared the values in the CJIS electronic spreadsheets to a number of sources. First, we tested the completeness of the LEO requisitions in the CJIS spreadsheets with the LEO requisitions in the BEARS database. Because BEARS was not in use until 2002, we did not expect the LEO requisitions in BEARS to contain all of the CJIS requisitions contained in the LEO spreadsheets. We did expect that all of the LEO requisitions coded in BEARS to be present in the CJIS electronic spreadsheets. Our review of the 86 LEO requisitions in BEARS showed, however, that 10 requisitions were not included in the CJIS spreadsheets. The invoiced amounts associated with these 10 requisitions were less than 1 percent of the total invoiced amount in BEARS of $41 million. The following table shows the requisitions related to LEO in BEARS.

[30] BEARS is a stand-alone system used to track requisitions more easily and in greater detail than is possible using the FBI's core financial system, FMS.

LEO-Related Requisitions CJIS BEARS Database

Requisitions	Number of Requisitions	Invoiced Amounts Associated with Requisitions
Included in the CJIS spreadsheets	76	$ 40,635,330
Not included in the CJIS spreadsheets	10	$ 274,001
Total	**86**	**$ 40,909,331**

Source: CJIS Financial Management Unit

We asked the CJIS Financial Management Unit to explain why all 86 requisitions were not included in its spreadsheets, and were told that 9 of the 10 requisitions totaling $150,421 in invoiced amounts related to office furniture and office equipment supporting the LEO program, but were not part of the LEO IT infrastructure.

CJIS Financial Management Unit officials told us the last requisition related to LEO – $123,580 paid to an FBI contractor – should have been captured in spreadsheets and included in the costs reported for CPIC purposes. Officials also told us the expenditure related to this requisition was paid from CJIS funding not designated for the LEO project, which explains why it was incorrectly excluded.

We next obtained a listing from FMS of all payments made to LSU since October 1999.[31] This listing contained 387 payments totaling $45,813,271. With the help of the CJIS Financial Management Unit staff, we attempted to reconcile the payments from FMS with the requisitions contained in the LEO spreadsheets. The reconciliation proved to be difficult because the CJIS spreadsheets track requisitions and FMS data is based on payments. Because one requisition may result in a number of payments, we did not independently research each of the hundreds of payments.

However, from a limited review of some of the FMS-listed payments, we identified five requisitions related to LEO totaling $850,000 that were not included in the CJIS cost spreadsheets. Although our review was limited, it clearly demonstrates that not all

[31] FMS data prior to FY 2000 has been archived and retrieving this data took more time than our analysis permitted.

LEO-related costs have been captured by CJIS or reported in the OIG questionnaire.

We contacted LSU to collect any information it maintained on LEO to compare the costs provided by the FBI. The LEO Director at LSU provided this data and informed us of other activities related to LEO that the FBI has funded. LEO activities funded by the FBI include the InfraGuard, the Hostage Barricade System (HOBAS) and Bomb Data Center (BDC), the National Center for Missing and Exploited Children (NCMEC), the Katrina Fraud Task Force (KFTF), and the Law Enforcement Linguistic Access (LELA) system at LSU.[32]

We grouped the requisitions contained in the CJIS spreadsheets by their descriptions to compare them to the amounts provided by LSU as follows.

Comparison of LSU and CJIS Cost Data Related to Contracted Activities FYs 1995 through 2005

Activity	LSU Amount	CJIS Amount	Difference
Cooperative Agreement	$ 72,716,134	$ 62,349,855	$ 10,366,279
InfraGuard	$ 9,282,571	$ 7,850,850	$ 1,431,721
HOBAS and BDC	$ 1,710,086	$ 854,926	$ 855,160
NCMEC	$ 1,273,169	$ 1,195,916	$ 77,253
KFTF	$ 639,745	$ -	$ 639,745
LELA	$ 316,594	$ 163,572	$ 153,022
Total	**$ 85,938,299**	**$72,415,119**	**$ 13,523,180**

Source: OIG analysis

Similar to the difficulty we had comparing the amounts in FMS based on payments to the amounts in the CJIS spreadsheets based on requisitions, LSU's costs are based on amounts invoiced to the FBI.

We asked the CJIS Financial Management Unit to explain the differences in the two sets of costs. Although officials pointed to the possibility of timing differences between the CJIS and LSU data, they acknowledged timing issues alone cannot explain these significant differences. Instead, CJIS Financial Management Unit officials told us the bulk of these differences appear to be attributable to transactions

[32] See Appendix V for more information on these activities.

with LSU made by other FBI components, not by CJIS. Although CJIS manages LEO and all CJIS requisitions are included in the CJIS BEARS database, funding for LEO projects can come from outside CJIS. The spreadsheets maintained by CJIS included amounts for LEO related to non-CJIS FBI components, but the CJIS Financial Management Unit can only track non-CJIS requisitions and payments when informed of them. We did not attempt to reconcile the LSU and CJIS amounts because CJIS officials did not believe the differences could be reconciled.

To calculate the FTE costs for LEO, CJIS Financial Management Unit staff obtains data from the Bureau Personnel Management System.[33] The Human Resources Division uses the Bureau Personnel Management System to capture and manage data on FBI personnel. The Bureau Personnel Management System tracks FBI employee information including salary information and the cost code to which they are assigned.[34] CJIS officials told us that employees working with LEO are assigned one of three different codes. One of these codes includes employees assigned to LEO as well as another FBI IT system. After checking with administrative staff working for the LEO program, CJIS Financial Management Unit staff adjusted the list of employees to include only those working on LEO. The salaries of those employees determined to be working on LEO is then totaled.

For FY 2005, the FBI salaries related to LEO amounted to $2,323,795. To this amount the CJIS Financial Management Unit applied the fringe benefit rate of 32.8 percent prescribed by OMB, and the resulting total amount of LEO FTE costs for FY 2005 was reported as $3,086,000.

To test these FTE costs, we reviewed the Bureau Personnel Management System's current listing of employees and their salaries for the three cost codes related to LEO. According to the Bureau Personnel Management System, there are 34 employees assigned to the three LEO-related cost codes with a combined salary of $2,502,314.

---

[33] The CJIS Financial Management Unit staff uses Bureau Personnel Management System data and follows the method described above for LEO and other projects they consider small. Larger CJIS projects, such as the Integrated Automated Fingerprint Identification System, use an Activity Based Cost model. After the number of FTEs is identified, personnel cost rates provided by the FBI's Finance Division are used to calculate total personnel costs.

[34] The cost codes used by the Bureau Personnel Management System are the same used by FMS.

Although the current combined salary amount in the Bureau Personnel Management System for the three cost codes is 8 percent higher than the reported LEO amount in FY 2005, we do not believe this, by itself, indicates reported costs are understated. Instead, the relatively small difference may be attributable to the following causes:

- Current salary amounts likely include employees not assigned to LEO;
- Staffing changes since FY 2005 would result in changes in salaries; or
- Increases in salaries would extend across the government.

In addition to our analysis using the Bureau Personnel Management System, we asked the LEO Director at LSU to provide the number of FBI employees working on LEO. She estimated that during FY 2005, approximately 30 FBI employees worked full time on LEO-related tasks.

Finally, as shown in the following table, we compared the costs reported for LEO in the CJIS Financial Management Unit spreadsheets with the outlays for LEO in OMB's eCPIC database.

LEO PMO and eCPIC Cost Data
FYs 1995 - 2005
($ in millions)

Costs	Amounts Per PMO	Amounts Per eCPIC	Difference
Non-personnel[a]	$ 85	$ 101	$ 15
FTE costs	$ 30	$ 30	-
Total[a]	**$ 115**	**$ 130**	**$ 15**

Source: CJIS and DOJ documents

[a] Due to rounding, not all values sum.

As shown in the table above, FTE costs were the same in both the CJIS spreadsheets and eCPIC database. However, the non-personnel amount in eCPIC was nearly $15 million more than the amount in the CJIS spreadsheets. We discussed this difference in reported non-personnel costs with the FBI CIO official responsible for

entering the data in eCPIC.[35] The official confirmed that the CIO's records showing the same amounts reported by CJIS and the eCPIC non-personnel amount was incorrect. The official explained that the eCPIC value is incorrect because the FBI did not update prior year outlays for LEO and some other FBI IT systems during the last budget cycle. The FBI updated the prior year outlays for only those 16 systems it considers major systems. The official also explained that prior year costs for LEO and many other systems were not updated in eCPIC because of the CIO's limited staff and resources.

In summary, the CJIS Financial Management Unit maintains records that provide reasonable assurance that the amounts reported in the OIG questionnaire can be verified. However, we determined these records do not capture all FBI costs related to LEO. From FMS payment data and LSU records, we determined the FBI investment in the LEO project could be as much as $13 million more than the $115 million reported.

DEA Concorde

Concorde is a DEA IT system designed to integrate DEA's IT functions, improve business processes, and enable information sharing within the component. It is intended to allow Special Agents, Intelligence Analysts, and other investigative professionals to manage investigative case files digitally. The central feature of the Concorde system is the Investigative Management Program and Case Tracking System (IMPACT), a web-based case management system.

The DEA's response to our request for Concorde cost information showed that the program began in 2000, with related costs through FY 2005 totaling $19.8 million. The DEA also reported government FTE costs amounting to $3.7 million, with five contractors individually paid at least $1.3 million over this same period. The following table presents a selection of the cost data DEA initially provided.

[35] Although eCPIC is accessible from most federal agencies' intranet systems, this is not the case at the FBI. Instead, the FBI's CIO Investment Management Unit collects and enters the data for the individual IT systems into eCPIC.

Concorde Reported Costs FYs 2000-2005
($ in millions)

Costs associated with 5 largest contractors	$	13.1
Personnel - DEA FTEs	$	3.7
Other contracted costs	$	3.0
Total Costs	**$**	**19.8**

Source: OIG analysis of completed Concorde questionnaire

We met with DEA officials to review their cost-tracking methods and supporting documentation, and analyzed the cost information provided. After we requested that DEA ensure the cost data extended back to the beginning of the Concorde project, DEA officials provided information noting that the program was conceived in 1997 with the name "UMBRELLA." DEA officials told us the goals of UMBRELLA were the same as Concorde and only the name had changed.

DEA officials also provided us with copies of the PMO electronic spreadsheets they used to track Concorde's contracts and related invoices since FY 2000. The following table presents Concorde's contract-related expenditures between FYs 2000 through 2005.

Concorde Contract Invoices
FYs 2000 - 2005

Fiscal Year		Amount
2000	$	947,510
2001	$	1,891,135
2002	$	3,729,187
2003	$	3,698,410
2004	$	4,843,233
2005	$	741,749
Total[a]	**$**	**15,851,226**

Source: Concorde invoice detail

[a] Due to rounding, values do not sum.

Although we previously determined that the DEA's financial system, the FFS, is not organized in such a way to easily and reliably identify all the costs associated with any particular IT system, DEA

finance staff told us a unique code to track funding for Concorde was created in FY 2005. Prior to 2005, Concorde did not have a defined allocation within the DEA's budget.

DEA finance staff provided us with an FFS report that captured all activity associated with the Concorde fund code in FYs 2005 and 2006. To the extent possible, we tested the completeness of the Concorde PMO spreadsheets by using this FFS report. Although the report tracks the use of Concorde funding allotment within the DEA budget, it does not necessarily capture all costs related to Concorde. From the PMO spreadsheets, we identified costs related to Concorde that were funded from DEA sources other than the Concorde budget allotment. DEA officials told us these other sources funded Concorde as well a number of other projects.

The following table presents the amounts in FFS related to Concorde funding for operations and equipment during FYs 2005 and 2006.

Amounts Expended from Concorde Funding in DEA Budget
($ in millions)

Fiscal Year	Operations	Equipment	Total
2005	$ 4.379	$ 0	$ 4.379
2006	$ 1.870	$ 0.068	$ 1.938
Total	**$ 6.249**	**$ 0.068**	**$ 6.317**

Source: DEA

We analyzed the detail of the FFS amounts above and compared them with the PMO spreadsheets. From this analysis, we identified 19 task orders with invoiced amounts of $717,581 that were not included in the PMO spreadsheets. We determined that 13 task orders totaling $15,027 were for relatively small DEA travel and credit card expenditures. These amounts were not included in the reported costs because the PMO spreadsheets include only contracted activity. However, the remaining $702,555 in expenditures were related to Concorde contracts and should have been included in the PMO spreadsheets. DEA officials told us the incomplete project management cost data may have resulted from the accounting treatment for Concorde's software, which requires such costs to be reported as an asset in DEA's financial statement throughout the development phase rather than as an expense.

We considered testing the completeness of the $13.095 million associated with Concorde's major contractors by obtaining payments to these contractors from FFS. However, DEA finance staff informed us that these particular contractors performed a large volume of services for the DEA, of which Concorde is only a relatively small portion. DEA staff said they could not readily identify those payments specific to Concorde.

We next evaluated the government FTE costs of $3.7 million reported by DEA in our questionnaire. This amount reflects all DEA personnel costs since FY 2000 and translates to approximately five FTEs per year. DEA officials provided us with a spreadsheet used to estimate Concorde FTE costs. This spreadsheet included estimates for FYs 2003 through 2020. Total estimates are calculated by identifying the number of FTEs in each of eight job categories and multiplying this number by the amounts for salaries and benefits related to each category. In addition to salary and benefits, the FTE spreadsheets include estimated amounts for other DEA employee expenses, such as training and travel. The following table presents the Concorde FTE cost data from FYs 2003 to 2005.

Concorde FTE Cost Data
FYs 2003 - 2005

Fiscal Year	Number of FTEs	Salary & Benefits	Other FTE Expenses	Total
2003	4.8	$ 93,218	$ 24,032	$ 562,800
2004	5.3	$ 93,218	$ 24,032	$ 619,080
2005	5.0	$ 97,040	$ 24,032	$ 610,202
Annual Average	5.0			$ 597,361

Source: DEA

The DEA did not have this type of information available for any years prior to FY 2003. However, we used the average annual FTE costs from the table above to estimate the FTE costs from FYs 2000 through 2005. The total FTE costs we estimated – $3,584,165 – is only 3 percent less than the FTE costs of $3,703,000 the DEA reported.

Although this analysis suggests that the FTE costs reported by the DEA for Concorde are supportable, these amounts are not based on actual results. DEA officials told us they have no procedures for

tracking the time employees spend working on any particular project and the FTE costs are essentially estimates. In addition, the DEA does not have a time utilization tracking system that would identify the actual time spent on Concorde-related activities for all job categories.

Because the Concorde program began in 1997 and the earliest cost data we reviewed was for FY 2000, we asked DEA officials to provide any additional spreadsheets or cost data they could identify with this data. Officials provided us with past IT spending plans for FYs 1998 and 1999 showing Concorde total obligated costs of $770,000.[36]

Finally, we obtained from DOJ's OCIO the reported amounts for Concorde contained in OMB's eCPIC database. The following table compares these amounts with the amounts contained in the PMO spreadsheets already discussed.

Concorde PMO and eCPIC Cost Data
Excluding Government Personnel Costs
FYs 2000 – 2005
($ in thousands)

Fiscal Year	Amounts per PMO	Amounts per eCPIC	Difference
2000	$ 948	-	$ 948
2001	$ 1,891	-	$ 1,891
2002	$ 3,729	$ 5,730	$ 2,001
2003	$ 3,698	$ 5,634	$ 1,936
2004	$ 4,843	$ 3,576	$ 1,267
2005	$ 742	$ 5,634	$ 4,892
Total	**$ 15,851**	**$ 20,574**	**$ 4,723**

Source: DEA and DOJ officials

We asked DEA officials to explain the significant differences between these two amounts' sources. Although the eCPIC data appears to represent prior years actual outlays, the DEA official responsible for entering IT system data into eCPIC told us this is not the case. He explained that budget estimate amounts from the start of the year are often used to report the outlays at the end of the year.

[36] The FY 1998 IT spending plan includes FY 1997 obligations for Concorde. The total obligated costs of $770,000 reflects FYs 1997 through 1999.

The DEA does not routinely report actual amounts for prior year outlays because they view eCPIC as a planning tool, where the emphasis is placed on estimated future amounts, not costs previously incurred.

In summary, the Concorde costs we reviewed did not include all program costs since inception. We identified approximately $700,000 in software–related expenditures missing from project cost sheets, and another $770,000 of expenditures from the first 2 years of program that were not reported. In addition, Concorde's actual reported FTE costs are estimated at the beginning of each year. In our view, the true costs of Concorde should include all costs incurred since 1997 when Concorde began.

JMD Justice Consolidated Office Network

JMD's Justice Consolidated Office Network (JCON) is the common office automation platform that over 70,000 employees from 16 DOJ components use daily. JCON provides the IT tools and services that allow these employees to perform their computer-based work duties.[37] Specifically, the JCON provides the basic IT computing framework for DOJ, which includes hardware such as networked workstations and printers, and applications such as e-mail and word processing. JCON also provides the infrastructure for components to access other IT systems such as case management databases and DOJ's Financial Management Information System.

The JCON program is a partnership between the program management office (PMO) and the 16 DOJ components that rely on JCON. In this partnership, the PMO is responsible for funding and implementing all aspects of JCON planning and deployments, including acquiring hardware and software for the related components. The components themselves are responsible for and fund the operations and maintenance of these assets.

In response to our questionnaire, JCON PMO officials provided the cost information presented in the following table.

[37] The amounts discussed below represent JCON Planning and Acquisition only. JCON maintenance is funded by the 16 participating DOJ components.

JCON Costs
($ in millions)

FY Start	Costs incurred through FY 2005	Estimated Funding through FY 2009	Total Costs FY 2001 - FY 2009
2002	$ 193.567	$ 270.079	$ 463.646

Source: OIG analysis of completed JCON questionnaire

The JCON response also included the following information:

- Costs related to a single contractor account for $49,626,912 of the $193.6 million in costs incurred through FY 2005.
- Reported costs do not include the components operation and maintenance costs.
- Reported costs are associated with the "current standard architecture," called JCON IIA.
- Forecasts of funding requirements past FY 2009 have not yet been developed.

We requested the amounts paid to BAE Systems, the single largest contractor that provides full life cycle support services for JCON, so we could verify these costs from a source independent of the PMO. Using the BAE's tax identification number, we requested a listing of all payments made to the contractor from the JMD Finance staff. From a listing of payments made containing over 1,400 transactions totaling more than $149 million, we identified 504 payments related to JCON between FYs 2002 and 2005 totaling $49,537,777. The difference between the value we calculated and the value reported by JCON is $89,135, or less than 1 percent of the reported costs.

We met with JCON PMO staff to discuss the potential for using financial system and budget execution data to verify the remaining reported costs through FY 2005. We previously determined the various DOJ financial systems would not be able to identify the costs associated with all of the IT systems in the inventory. We discussed financial issues further with the JCON PMO and learned it would be possible in this case to create a report from the financial system that could identify planning and acquisition-related costs for JCON. The JCON PMO then prepared a JMD financial system (FMIS) report that

matched the $193.567 million it reported on our questionnaire. JCON officials told us this amount included the government FTE costs incurred over the period.

From our discussions with the JCON PMO, we also learned that in FYs 2004 and 2005, JCON planning and acquisition costs were funded entirely from the Legal Activities Office Automation appropriation. Because JCON planning and acquisition in the CPIC process was essentially the same as the Legal Activities Office Automation appropriation in the budget process, we compared the costs from these two processes. First, we matched the FY 2005 Exhibit 53 amount for JCON of $39.967 million with the $40 million reported for the Legal Activities Office Automation appropriation. Both these amounts reflect the budget authority. We then compared the amount of outlays for planning and acquisition in the Exhibit 300 with the same amount reported for the Legal Activities Office Automation appropriation in FY 2005. The Exhibit 300 reported about $49 million in outlays for FY 2005, while the President's Budget included outlays of $43 million for the same period – a difference of over $6 million.

We asked JCON officials about this discrepancy, and were told the $49 million included in the Exhibit 300 represented appropriations instead of outlays. We confirmed that the President's Budget reported $49 million for obligations in FY 2005 and asked JCON officials why outlays were not provided as required by OMB Circular A-11. JCON officials explained that they began reporting obligations because it was difficult to retrieve data on outlays from the previous version of the FMIS. To be consistent and avoid reporting the same cost twice, the JCON PMO continued reporting obligations rather than outlays.

In addition to the comparison of FY 2005 CPIC and budget data, we compared the $246 million total amount reported in the JCON Exhibit 300 for planning and acquisition to the $193.6 million total amount reported in the OIG questionnaire. JCON officials told us total costs in the Exhibit 300 costs were $53 million more than total costs reported to the OIG because the Exhibit 300 included expenditures from FY 2000 and 2001 and were not considered part of JCON IIA.

We researched government and industry sources for more information on JCON and JCON contracts. This search identified a $500 million JCON contract awarded in 1996, more than 5 years before the first costs reported in our questionnaire. Although the JCON PMO response made clear that the reported costs related to JCON IIA, we consider the JCON initiative to have begun in 1996 when

the decision was made to replace a collection of separate office automation systems with a consolidated DOJ platform.

The JCON PMO confirmed that the first attempt at replacing the existing office automation systems, known as JCON I, began in 1996 and was terminated in 1998 when it did not work. JCON II followed and evolved into JCON IIA by FY 2002. Because the earlier JCON efforts predate the current JCON Project Manager and other staff, they were not able to provide us with the complete costs of JCON prior to FY 2002.

Although JCON has not yet developed cost estimates for FYs 2010 through 2012, the JIST Budget Officer told us that funding in these years is expected to equal at least the FY 2009 level of $89.5 million.

In summary, by using financial system and budget data we were able to verify the costs the JCON Project Management Office reported to us. However, the Project Management Office said the costs only represent the current standard architecture. Although JMD views the various versions of JCON as separate systems, we believe the true cost of JCON should include all costs incurred since 1996 when the JCON project was initiated. Therefore, we conclude that JCON's costs since 1996 should be at least $53 million more than the $193.6 million we verified. In addition, because complete cost data was not available for JCON prior to FY 2002, we were unable to determine what amounts, if any, were paid in connection with the 1996 $500 million contract.

CIOs' Role in IT Spending and Budgeting

Although the DOJ CIO and component CIOs have significant responsibilities for their organization's IT systems, we found they have varying degrees of control over IT system budgets.

CIOs Control of IT Spending

In testing the completeness of reported costs for selected IT systems, we found that the control of IT spending and budgets by component CIOs varies. The FBI CIO's control over IT spending has increased over the last few years. In 2004, the FBI reported in its first IT Strategic Plan that its CPIC process and IT spending were not

centrally managed. However, the budget for the CIO now includes nearly 50 percent of the FBI's IT spending, and the CIO also has approval authority for IT spending not within the CIO's budget. This change since 2004 indicates more centralized management of the FBI's IT budget within the CIO's office.

At the DEA, the CIO controls approximately 60 percent of the agency's budgets relating to IT spending, and other DEA managers control the remainder. To help oversee DEA IT projects, the DEA CIO has created an Integrated Project Review process that allows the CIO to:

- conduct oversight of IT projects' progress toward costs and schedule milestones;
- evaluate IT system project managers;
- identify, as early as possible, cost, schedule, and performance slippages using Earned Value Management where appropriate;
- allocate limited CIO budget resources; and
- identify and share cross-cutting solutions, lessons learned, and common concerns.

While the Integrated Project Review is used for IT systems utilizing CIO funding, the Major Investment Review is used for any major DEA IT system using DEA funds or personnel. The objectives of the Major Investment Review are similar to those for the Investment Project Review.

At JMD, the creation of the JIST appropriation has given the CIO budget control over five of the six JMD IT systems in our inventory. Based on our discussion with the JIST Budget Officer, the CIO should have reliable cost data in future years.

Costs of DOJ IT Systems Contained in OMB eCPIC Database

Although the CIOs at the FBI, DEA, and JMD control the budgets of many IT systems, employ tools that monitor current spending, and review future year spending requests, we found the CIOs are generally unable to identify or verify all prior costs related to individual IT systems.

As part of our testing during this audit, we examined the prior years' cost data contained in the OMB eCPIC database. OMB uses eCPIC to collect cost and other data on individual IT systems. Of particular interest for this audit were the amounts contained in eCPIC for prior year outlays of the three IT systems we tested. In all three cases, we found the eCPIC prior year amounts were different from the amounts we tested in the OIG questionnaire, which indicates the eCPIC costs are inaccurate.

At the three components, we discussed with IT system project managers and CIO staff the differences between the eCPIC and questionnaire data. For each component, we determined a different cause behind these cost differences. In our view, it is critical for the adequate oversight of DOJ IT systems and projects that complete and accurate cost data be available on an individual system basis.

At the FBI, we determined that the CIO had stopped updating the prior year outlays for some IT systems, including LEO. For the DEA, we determined the CIO staff had not entered the actual outlay amount but instead used budgeted amounts. For JCON, we determined the difference in prior year questionnaire data related to the PMO's use of obligations rather than outlay data. In addition, we found that total costs extended 2 years further back than the data we initially were provided.

We also learned that each of the CIO staffs do not have a formal verification process of the prior year amounts reported by the PMOs for inclusion to eCPIC. OMB's eCPIC is also used by DOJ's OCIO to prepare the Exhibit 53.

Consistent with the President's Budget, the Exhibit 53 shows the appropriated amounts associated with individual DOJ IT systems.[38] The Exhibit 53, in effect, extracts and provides detail on amounts for IT spending already included in an agency's overall budget. According to OMB Circular A-11, an agency's Exhibit 53 must be fully integrated with that agency's overall budget submission. In addition, agencies must update each Exhibit 53 and the accompanying Exhibits 300 to reflect any changes due to final budget decisions.

[38] DOJ's Exhibit 53 summarizes office automation and infrastructure IT systems in the Consolidated Enterprise Infrastructure.

We discussed with officials at the JMD OCIO the extent to which the Exhibit 53 amounts could be traced to the component's overall budgets and financial systems. These officials told us the two documents are not completely integrated, but the OCIO is working with DOJ budget staff and the components on this issue.

Other Congressional Requests for IT System Costs

During our audit, the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security of the Senate Committee on Homeland Security and Governmental Affairs held hearings on federal IT projects at risk. Following this hearing, the Subcommittee asked all major federal agencies to list all of their on-going IT projects and whether they had experienced cost overruns. In response to this request, DOJ provided data on its IT systems, including the three IT systems we tested – LEO, Concorde, and JCON. The following table compares the responses to our questionnaire and the responses to the Subcommittee's request.

DOJ Responses to IT System Cost Inquiries Made by Senate Subcommittee and the OIG
($ in millions)

IT System	Senate Subcommittee's Request as of 10/2006	OIG Questionnaire as of 9/2005
LEO	N/A	$ 114.5
Concorde	$ 25.1	$ 19.8
JCON	$ 65.3	$ 193.6

Source: Senate Subcommittee's request and OIG questionnaire

Although we did not expect the amounts reported to the Senate Subcommittee and the OIG to exactly match due to the difference in reporting dates, the amounts for LEO and JCON did not appear to be consistent.

The FBI included a comment in the response to the Senate Subcommittee indicating that LEO is not an ongoing project, and FY 2006 development, modernization, and enhancement DME funds were

used for tactical enhancements only. We discussed this issue further with LEO and other FBI officials. They told us their initial response was made in error, and said they subsequently amended the response to be consistent with the information provided to us.

Although the amounts reported by the DEA for Concorde appeared consistent, the DEA indicated to the Senate Subcommittee that Concorde began in 1998, while we were initially provided cost data only as far back as 2000. Subsequently, the DEA confirmed a 1997 start date and provided us with the cost data for the years omitted from their initial response to us.

We discussed the difference in the JCON amounts with JMD officials, who told us the amounts reported to the Senate Subcommittee were taken from Earned Value Management data on the current baseline and included JMD as well as the component's share of JCON costs.

Conclusion

We concluded that the actual costs of DOJ IT systems that are provided to Congress, OMB, and senior management within DOJ, including the CIO, are unreliable. IT system cost reporting within DOJ is fragmented, uses inconsistent methodologies, and lacks control procedures necessary to ensure that cost data for IT systems is accurate and complete. Furthermore, DOJ does not have complete cost data for the three IT systems we tested and, based on our testing and other audit work, we lack confidence in the cost data reported for DOJ IT systems in general. We determined that the $327.9 million combined costs reported for these three systems was understated by at least $68 million. In our opinion, the lack of complete cost data that is verifiable for DOJ's IT systems compromises the effectiveness of DOJ's IT oversight entities, including Congress, OMB, the DIRB, and DOJ and component CIOs.

Although the primary purpose of DOJ's CPIC processes is IT planning and less emphasis is placed on prior years' costs, we believe it is important that the cost data used by decision-makers is reliable. Our audit casts doubt on the reliability of the data that DOJ components report to the CIO, the DIRB, OMB, Congress, and other oversight entities.

Recommendations

We recommend that the Assistant Attorney General for Administration:

1. Ensure that component CIOs develop and implement cost effective means to report accurate, complete, and verifiable costs for individual IT systems.

2. Ensure that DOJ's CIO improves the integration of the Exhibit 53 and budget submissions in accordance with OMB Circular A-11 so that Exhibit 53 amounts can be traced to the components' overall budgets and financial systems.

3. Assess the feasibility of using the DOJ's planned Unified Financial Management System for Capital Planning and Investment Control cost reporting.

Statement on Compliance with Laws and Regulations

In response to the conference report for the FY 2006 Science, State, Justice, Commerce, and Related Agencies Appropriations Act (P.L. 109-108), we audited information concerning DOJ's major IT systems. The audit was conducted in accordance with the *Government Auditing Standards*. As required by the standards, we reviewed management processes and records to obtain reasonable assurance that DOJ's compliance with laws and regulations that could have a material effect on DOJ operations. Compliance with laws and regulations applicable to DOJ's IT systems is the responsibility of DOJ's Office of Chief Information Officer management.

Our audit included examining, on a test basis, evidence about laws and regulations. The specific laws and regulations against which we conducted our tests are contained in:

- Clinger-Cohen Act of 1996
- Office of Management and Budget Circular A-11

Our audit identified no areas where DOJ was not in compliance with the laws and regulations referred to above. With respect to those transactions not tested, nothing came to our attention that caused us to believe that DOJ management was not in compliance with the laws and regulations cited above.

Statement on Internal Controls

In planning and performing our audit of DOJ's IT systems inventory, we considered DOJ's internal controls for the purpose of determining our audit procedures. This evaluation was not made for the purpose of providing assurance on the internal control structure as a whole. However, we noted certain matters that we consider to be reportable conditions under the *Government Auditing Standards*.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal control structure that, in our judgment, could adversely affect DOJ's ability to manage its IT systems. During our audit we found the following internal control deficiency.

- DOJ does not have in place a means to report accurate, complete, and verifiable costs for its major IT systems.

Because we are not expressing an opinion on DOJ's internal control structure as a whole, this statement is intended solely for the information and use of DOJ in managing its IT investments. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

APPENDIX I

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The conference report for the FY 2006 Science, State, Justice, Commerce, and Related Agencies Appropriations Act (P.L. 109-108) directs the OIG to: (1) produce an inventory of DOJ's major IT systems and planned initiatives, and (2) report on the effectiveness of DOJ's IT planning efforts. This audit report responds to the congressional request to compile an inventory of DOJ's major IT systems.

The objective of this audit was to produce an inventory of DOJ's major IT systems and planned initiatives, and provide the system name, system description, DOJ component owner, cost, and implementation status.

Scope and Methodology

The audit was performed in accordance with the *Government Auditing Standards*, and included tests and procedures necessary to accomplish the audit objectives. We conducted field work at JMD OCIO facilities and FBI headquarters in Washington, D.C., as well as the DEA headquarters in Arlington, VA. In addition, we conducted work at the FBI Criminal Justice Information Services Division in Clarksburg, West Virginia.

We interviewed officials from DOJ, the FBI, DEA, ATF, and BOP. At the component level we interviewed officials in their OCIOs and finance departments. We also interviewed the program managers for the FBI's Law Enforcement Online, DEA's Concorde, and JMD's Justice Consolidated Network.

We reviewed documents related to DOJ and components' IT oversight, ITIM and CPIC policies, financial systems, financial statements, budget processes, and IT system cost data. In addition, we reviewed relevant laws, congressional testimony, and prior OIG and GAO reports.

To identify major DOJ IT systems, we reviewed congressional, OMB, and DOJ documents listing DOJ IT systems as major or high-risk. We included those IT systems that Congress identified in the Science,

State, Justice, Commerce, and Related Agencies Appropriations Act of 2006. Likewise, we included in the inventory the IT systems with Exhibits 300. We also included the DOJ IT systems on OMB's High Risk Project list, all the IT systems reviewed by the DIRB, several IT systems shown on the OCIO Dashboard, and systems requiring Earned Value Management.

We used OMB Exhibits 53 and Exhibits 300 along with DOJ documents to provide descriptions of the IT systems.

To obtain the cost of the IT systems, we first asked component finance staffs to provide us IT system costs from their financial systems. The components explained that their financial systems do not report by individual IT system. We also requested CIO staffs to provide us with independent cost information, but they too do not have the ability to provide individual IT system cost data.

We therefore distributed a questionnaire to all 38 major IT system managers requesting total system costs from inception to September 30, 2005. We also requested in the questionnaire funding projections through FY 2012 for the IT systems. We then selected three systems to test the reliability and completeness of the costs provided to us.

DOJ officials provided us with the implementation status for each IT system. Using Federal Information Security Management Act information, the FBI provided us with implementation status of its IT systems.

APPENDIX II

MAJOR IT SYSTEMS & PROJECTS

Table A. Conference Report to FY 2006 Science, State, Justice, Commerce and Related Agencies Appropriations Act

	Component	Phase II System
1	JMD	Integrated Wireless Network
2	JMD	Unified Financial Management System
3	JMD	Public Key Infrastructure
4	ATF	National Integrated Ballistics Information Network
5	FBI	Integrated Automated Fingerprint Identification System
6	FBI	Sentinel
7	FBI	Terrorist Screening Center
8	FBI	Next Generation Integrated Automated Fingerprint Identification System
9	FBI	Law Enforcement National Data Exchange
10	FBI	Regional Data Exchange
11	FBI	Law Enforcement Online
12	FBI	Sensitive Compartmented Information Operational Network
13	FBI	Biometric Reciprocal Identification Gateway/Criminal Justice Information Sharing Interoperability Initiative

Source: P.L. 109-108

Table B. DOJ's OMB Exhibits 300

	Component	Phase II System
1	JMD	Litigation Case Management System
2	JMD	Unified Financial Management System
3	OJP	Grants Management System
4	EOIR	eWorld
5	BOP	BOP Inmate Telephone System-II
6	FBI	Integrated Automated Fingerprint Identification System
7	FBI	Sentinel
8	FBI	Terrorist Screening Center
9	FBI	National Instant Criminal Background Check System
10	FBI	Next Generation Integrated Automated Fingerprint Identification System
11	FBI	Digital Collection
12	FBI	National Crime Information Center
13	FBI	Foreign Terrorist Tracking Task Force
14	FBI	Law Enforcement National Data Exchange
15	FBI	Electronic Surveillance Data Management System
16	FBI	Technical Refresh Program
17	FBI	Regional Data Exchange
18	FBI	Computer Assisted Response Team Storage Area Network
19	DOJ	Consolidated Enterprise Infrastructure

Source: DOJ Exhibits 300

Table C. DOJ Systems Requiring Earned Value Management

	Component	Phase II System
1	JMD	Integrated Wireless Network
2	JMD	Unified Financial Management System
3	JMD	Litigation Case Management System
4	JMD	Justice Consolidated Network
5	JMD	Public Key Infrastructure
6	DEA	Merlin
7	DEA	FIREBIRD
8	EOIR	eWorld
9	OJP	Grants Management System
10	FBI	Sentinel
11	FBI	Next Generation Integrated Automated Fingerprint Identification System
12	FBI	Law Enforcement National Data Exchange
13	FBI	Electronic Surveillance Data Management System
14	FBI	Law Enforcement Online
15	FBI	Sensitive Compartmented Information Operational Network
16	FBI	Biometric Reciprocal Identification Gateway/Criminal Justice Information Sharing Interoperability Initiative

Source: DOJ OCIO

Table D. DOJ and OMB Designated High-Risk Projects

	Component	Phase II Systems
1	JMD	Integrated Wireless Network
2	JMD	Litigation Case Management System
3	JMD	Unified Financial Management System
4	FBI	Sentinel
5	FBI	Terrorist Screening Center
6	FBI	Next Generation Integrated Automated Fingerprint Identification System
7	FBI	Law Enforcement National Data Exchange
8	FBI	Multi-Agency Information Sharing Initiative Regional Data Exchange

Source: U.S. Government Accountability Office. *Information Technology: Agencies and OMB Should Strengthen Processes for Identifying and Overseeing High Risk Projects,* Report Number GAO-06-647, June 2006.

Table E. Department Investment Review Board

	Component	Phase II Systems
1	JMD	Integrated Wireless Network
2	JMD	Unified Financial Management System
3	JMD	Litigation Case Management System
4	JMD	Classified Information Technology Program
5	JMD	Justice Consolidated Network
6	JMD	Public Key Infrastructure
7	DEA	OCDETF Fusion Center System
8	FBI	Integrated Automated Fingerprint Identification System
9	FBI	Sentinel
10	FBI	Terrorist Screening Center
11	FBI	Law Enforcement National Data Exchange

Source: DOJ Enterprise Architect

Table F. OCIO Dashboard Systems with 3-years' Cost Exceeding $15 million[a]

	Component	Phase II Systems
1	JMD	Integrated Wireless Network
2	JMD	Justice Consolidated Network
3	JMD	Litigation Case Management System
4	JMD	Unified Financial Management System
5	JMD	Public Key Infrastructure
6	DEA	FIREBIRD
7	DEA	OCDETF Fusion Center System
8	EOIR	eWorld
9	OJP	Grants Management System
10	FBI	Sentinel
11	FBI	Terrorist Screening Center
12	FBI	Next Generation Integrated Automated Fingerprint Identification System
13	FBI	Law Enforcement National Data Exchange
14	FBI	Electronic Surveillance Data Management System
15	FBI	FBI Security Management Information System
16	FBI	Multi-Agency Information Sharing Initiative Regional Data Exchange
17	FBI	Law Enforcement Online
18	FBI	Sensitive Compartmented Information Operational Network

Source: DOJ OCIO

[a] IT systems - JMD Classified Information Technology Program, DEA Merlin, FBI Investigative Data Warehouse, and FBI Computer Assisted Response Team Storage Area Network - are monitored by the OCIO dashboard. However, they do not have 3-year costs exceeding $15 million. These four systems were included in the inventory because they met additional criteria.

APPENDIX III

PRIOR REPORTS

In recent years, the Office of the Inspector General and the Government Accountability Office (GAO) have conducted several audits that are relevant to our review of DOJ IT systems. These audit reports resulted in many findings and recommendations to DOJ and component IT management, which focused on establishing and correcting existing IT investment management (ITIM) and Capital Planning and Investment Control (CPIC) structures. These reports did not audit the reliability of cost data for any specific projects.

Department of Justice, Office of the Inspector General

In December 2002, the OIG issued Audit Report 03-09, *The Federal Bureau of Investigation's Management of Information Technology Investments*, which reviewed the FBI's IT management processes and IT-related strategic planning and performance measurement activities. The OIG reported that the FBI did not meet the fundamental elements of a sound ITIM. The OIG also reviewed the FBI's management of Trilogy, the FBI's largest and most critical IT project at the time. The OIG found that the lack of critical IT investment management processes contributed to missed milestones and led to uncertainties about cost, schedule, and technical goals.

Although the FBI took steps to improve IT management, the OIG report concluded that the FBI's IT strategic planning and IT performance measurement were inadequate. Likewise, the FBI's strategic plan did not include goals for IT investment management, and the FBI's strategic plan and performance plan was not consistent with DOJ's annual performance plan.

In 2005, the OIG again looked at the FBI's IT structure – specifically the Trilogy IT project. The OIG issued Audit Report 05-07, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project*, to assess FBI's Trilogy project. In April 2004, the FBI had completed the infrastructure upgrade portion of the Trilogy project. However, at the time of the OIG audit the FBI was over budget and behind schedule for the Virtual Case File system of Trilogy. This report contained nine recommendations regarding the FBI's management of the remaining aspects of the Trilogy project and its IT management in general,

including one to ensure its financial systems could track Trilogy project costs accurately and completely.

The OIG has also reviewed enterprise architecture development and IT management at other DOJ components. In September 2004, the OIG issued Audit Report 04-36, *The Drug Enforcement Administration's Management of Enterprise Architecture and Information Technology Investments*. The OIG concluded that the DEA was effectively pursuing completion of both its enterprise architecture and ITIM. The OIG provided the DEA with seven recommendations for developing the enterprise architecture and ITIM.

In November 2005, the OIG issued Audit Report 06-02, *The Status of Enterprise Architecture and Information Technology Investment Management in the Department of Justice*. At the time of the OIG audit, DOJ had not yet established an Enterprise Architecture or ITIM processes and therefore was not in compliance with the Clinger-Cohen Act, OMB guidance, and DOJ regulations. However, DOJ was actively developing and implementing new frameworks aimed at establishing an Enterprise Architecture and ITIM processes. The OIG provided seven recommendations to JMD to improve DOJ's IT management.

Government Accountability Office

The GAO has also reviewed the FBI Trilogy Project and other issues concerning management of IT at DOJ. In February 2006, GAO issued *Federal Bureau of Investigation: Weak Controls over Trilogy Project Led to Payment of Questionable Contractor Costs and Missing Assets*, which identified millions of dollars in questioned costs and missing assets.

In 2005 and 2006, the GAO reviewed government-wide IT and the Office of Management and Budget's processes for overseeing these investments.[39] The GAO's reports reviewed IT systems identified as high-risk projects and those listed on OMB's Management Watch List. GAO concluded that OMB should develop single lists for both high risk

[39] Government Accountability Office. *Information Technology: OMB Can Make More Effective Use of Its Investment Reviews*, Report Number GAO-05-276, April 2005.

Government Accountability Office. *Information Technology: Agencies and OMB Should Strengthen Processes for Identifying and Overseeing High Risk Projects*, Report Number GAO-06-647, June 2006.

and Management Watch List projects and their respective deficiencies, and direct agencies to consistently apply the criteria for designating projects at high risk.

In 2005, the GAO completed an update to Congress on government-wide high-risk areas.[40] The GAO identified 25 high risk areas, which included managing federal real property and protecting the federal government's information system and the nation's critical infrastructure. Similar to what the OIG found in the current audit, the GAO determined the actual cost data for IT systems at other agencies was unreliable. Further, the GAO found these agencies relied on ad-hoc costing processes rather than formal cost accounting systems with adequate controls.

[40] Government Accountability Office. *High-Risk Series: An Update*, Report Number GAO-05-207, January 2005.

APPENDIX IV

MAJOR DOJ IT SYSTEMS – DESCRIPTION & IMPLEMENTATION STATUS

Component	IT System	Description	Implementation Status
FBI	Integrated Automated Fingerprint Identification System (IAFIS)	IAFIS provides fingerprint identification services for local, state, federal and international law enforcement community and homeland security.	Phase 8 – Operations & Maintenance
FBI	Next Generation Integrated Automated Fingerprint Identification System (NGI)	The NGI initiative will study the integration strategies and indexing of additional biometric data, which will support a futuristic multimodal system.	Phase 3 – Acquisition Planning
FBI	National Instant Criminal Background Check System	Provides criminal background checks in support of the Brady Act[a]	Phase 8 – Operations & Maintenance
FBI	National Crime Information Center (NCIC)	NCIC is an on-line information service managed by the FBI to provide a means for sharing criminal justice information about individuals, vehicles, and property associated with criminal activity.	Phase 8 – Operations & Maintenance

FBI	Law Enforcement Online Re-engineering/Relocate	LEO is a global virtual private network provided by the FBI to all levels of the law enforcement, criminal justice, and public safety communities, which provides secure dissemination of Sensitive But Unclassified information.	Phase 7 – Implementation & Integration
FBI	Law Enforcement National Data Exchange (N-DEx) Rev 9/7	The FBI's N-DEx initiative will develop a complex interactive information sharing network which implements the core platform for DOJ Law Enforcement Information Sharing.	Phase 4 – Source Selection
FBI	Combined DNA Index System (CODIS)	CODIS enables federal, state, and local crime labs to compare and exchange DNA profiles electronically, thereby linking crimes to each other and to convicted suspects.	Phase 3 – Acquisition Planning
FBI	Electronic Surveillance Data Management System	Involves 2 elements: (1) increasing the FBI's ability to manage, analyze, and share electronic surveillance, seized media and other types of collected data and (2) integrating data analysis capabilities that improve its efficiency.	Phase 8 – Operations & Maintenance
FBI	Investigative Data Warehouse	Investigative Data Warehouse is a concept describing the preparation and organization of a variety of databases so they can be searched in a coordinated fashion along with other databases.	Phase 8 – Operations & Maintenance
FBI	Biometric Reciprocal Identification Gateway/Criminal Justice Information Services Interoperability Initiative	Provide secure electronic connectivity to customers who access FBI's LEO services, IAFIS, NCIC, and CODIS.	Various
FBI	Computer Assisted Response Team Storage Area Network	Systems used to conduct forensic examinations of computers and computer related media in support of the FBI, intelligence organizations and other key law enforcement agencies.	Phase 2 – Requirements Development

FBI	Sentinel	Provides electronic case, records, workflow, evidence management, case tracking and records search and reporting capabilities that will replace the current paper-based case management system and its related supporting capabilities.	Phase 8 – Operations & Maintenance
FBI	Data Centers	The Data Centers' goals are to provide continuous, effective automated production workload support and business continuity for all FBI investigative and administrative missions.	Phase 8 – Operations & Maintenance
FBI	Technical Refresh Program	Provides for the technical refreshment of FBI Trilogy computing assets.	Phase 8 – Operations & Maintenance
FBI	Digital Collection	The Digital Collection Project enables the FBI in collecting evidence and intelligence to facilitate and support national security, domestic counterterrorism, and criminal investigative efforts.	Phase 8 – Operations & Maintenance
FBI	Multi-Agency Information Sharing Initiative Regional Data Exchange	Multi-Agency Information Sharing Initiative Regional Data Exchange will combine and share regional investigative information and provide powerful tools for analyzing the integrated data sets.	Phase 8 – Operations & Maintenance
FBI	Terrorist Screening Center	Terrorist Screening Center consolidates a terrorist screening database of domestic and international terrorists.	Phase 8 – Operations & Maintenance

FBI	Foreign Terrorist Tracking Task Force	The Foreign Terrorist Tracking Task Force is co-locating and managing data for end-to-end decisions that contribute to the mission of keeping foreign terrorists and their supporters out of the United States or lead to their exclusion, denial of benefits, surveillance, or prosecution.	Phase 8 – Operations & Maintenance
FBI	Security Management Information System	Integrates security into all business processes to protect FBI employees, information, operations, and facilities. Emphasizes information sharing and knowledge management to facilitate threat identification, risk mitigation, and incident prevention.	Phase 5 - Design
FBI	Information Assurance Technology Infusion	Designs and develops enterprise security solutions for FBI information systems.	Various
FBI	Sensitive Compartmented Information Operational Network	Provides Top Secret/Sensitive Compartmented Information capabilities including LANs, security measures, access authentication and control, file/print services, administrative directory services, desktop computers, and software.	Phase 8 – Operations & Maintenance
DEA	Model 204 Corporate Systems	The M204 system includes approximately 32 core investigative and administrative applications that support the DEA's mission, strategic goals, and objectives as well as serving specific needs of external DEA partners.	Operational
DEA	E-Commerce-Controlled Substances Ordering System	The E-Commerce-Controlled Substances Ordering System and the Electronic Prescriptions for Controlled Substances system will enable the safe electronic transmission of prescriptions and the electronic ordering of controlled substances.	Developmental

DEA	EPIC Information Systems	E-gov modernization of systems in this one-of-a-kind national repository for tactical law enforcement intelligence to federal, state, and local law enforcement.	Operational
DEA	Concorde	Concorde is the “To Be” e-gov solutions architecture that seamlessly performs all DEA re-engineered business processes. Initial focus is support to DEA investigations and information sharing.	Development
DEA	Firebird	Primary infrastructure enabling investigative case management and all other Sensitive But Unclassified information systems. The client-server based network links DEA offices and components worldwide and supports the full spectrum of DEA operations.	Operational
DEA	Merlin	Merlin provides the single point of connectivity between DEA offices for rapid transmission of, and access to, classified investigative and intelligence information.	Operational
DEA	Organized Crime & Drug Enforcement Task Force Fusion Center System	The OCDETF Fusion Center System will establish a single entity for drug and related financial investigative information.	Operational
JMD	Integrated Wireless Network	IWN is an interagency initiative that will provide a secure, tactical narrowband communications capability with required functionality, including interoperability to the law enforcement and homeland security agents in DOJ, Treasury and Homeland Security.	Operational
JMD	Unified Financial Management System	DOJ has initiated an effort to implement the UFMS, which will improve the existing and future financial management and procurement operations across DOJ.	Development

JMD	Litigation Case Management System	Litigation Case Management System is the first investment to emerge from the Case Management Common Solutions initiative and is focused on providing a common litigation case management solution for the seven DOJ litigating divisions.	Development
JMD	Classified Information Technology Program	Classified Information Technology Program will provide an enterprise-wide seamless IT infrastructure for electronically sharing, processing, and storing information classified at the Secret, Top Secret, and Sensitive Compartmented Information levels.	Implementation
JMD	Justice Consolidated Office Network	JCON is the critical infrastructure that provides a reliable and robust common office automation platform upon which 16 of DOJ's litigating, management, and law enforcement components operate their mission-critical applications.	Operational
JMD	Public Key Infrastructure	The Public Key Infrastructure will provide secure communications and information sharing inside and outside DOJ and enable rigorous identification and authentication of IT system users, to better protect DOJ sensitive and classified information and assets.	Implementation
ATF	National Integrated Ballistics Information Network	Facilitates sharing ballistic crime gun evidence information across jurisdictional boundaries allowing state and local law enforcement agencies to work together to prevent terrorism and violent crime.	Operational
BOP	Inmate Telephone System-II	Provides telephone calling service to and from inmates and provides recording of phone call services.	Operational

EOIR	eWorld	eWorld is a project that will enable EOIR to make the transition from paper to electronic documents for its official adjudication records, thereby increasing access and efficiency.	Operational
OJP	Grants Management System	Provides automated support in managing the application for and approval of federal grant funds. Grants Management System enables managers to track and monitor over 20,000 grants. It is a web-based, data driven application, giving access to applicants around the U.S.	Operational

Source: Description – OMB Exhibit 53 and Exhibits 300, and DOJ documents

[a] Brady Handgun Violence Prevention Act (P.L. 103-159)

APPENDIX V

DESCRIPTIONS OF THE LEO ACTIVITIES FUNDED BY THE FBI AT LSU

Hostage Barricade System

The Hostage Barricade System research project is part of the FBI's Critical Incident Response Group, and its purpose is to gather and analyze statistics on hostage, barricade, and suicide incidents in the United States.

Bomb Data Center

The Bomb Data Center is also located within the FBI's Critical Incident Response Group and its mission is to enhance the capabilities of FBI Special Agent Bomb Technicians, state and local bomb squads, and other federal agencies to respond to bombing incidents, terrorist threats, and special events security through intelligence sharing, training, and other resources.

Law Enforcement Linguistic Access

The FBI and other DOJ components, as well as the Intelligence Community, designed the Law Enforcement Linguistic Access system to maximize the use and availability of linguists who are currently on contract to any one of the partner agencies.

National Center for Missing and Exploited Children

The National Center for Missing and Exploited Children is a private, non-profit organization that operates under a congressional mandate and works in cooperation with DOJ's Office of Juvenile Justice and Delinquency Prevention. An FBI Supervisory Special Agent coordinates FBI and National Center for Missing and Exploited Children resources to facilitate the most effective FBI response to child abductions, parental kidnappings, and sexual exploitation of children.

Katrina Fraud Task Force

The Task Force includes the FBI and other DOJ components, other federal agencies, and various representatives of state and local law enforcement. The Task Force coordinates on the federal, state,

and local levels with law enforcement and with other entities involved in the relief and reconstruction effort related to Hurricane Katrina.

InfraGuard

InfraGuard is an FBI sponsored program that shares information and intelligence to prevent hostile acts against the United States. In addition to the FBI, InfraGard includes businesses, academic institutions, state and local law enforcement agencies, and other participants.[41]

[41] For presentation purposes we have included with InfraGuard, amounts for the National Infrastructure Protection Center. The National Infrastructure Protection Center was transferred from the FBI to Department of Homeland Security in 2003.

OTHER MATTERS

In the course of this audit, we identified concerns regarding DOJ's financial and budget systems and Capital Planning and Investment Control cost reporting. We believe that DOJ should consider these concerns as it develops its CPIC cost reporting function.

FBI Requisition Databases and CPIC Cost Reporting

Officials from various FBI divisions told us that tracking purchase requisitions and the resulting expenditures using FMS, the FBI's core financial system, is sometimes difficult and time-consuming. In order to make tracking requisitions faster and easier, these divisions have developed databases that duplicate and add detail to their requisitions in FMS.

The FBI has created and operates a number of requisition databases at many of its operating units. The CJIS Division was the first to create its requisition database, Budgetary Evaluation and Analysis Reporting System (BEARS) in 2002. Since 2002 other FBI divisions have adopted similar databases that are also called BEARS.

In addition to the various requisition databases using the name BEARS, the FBI Office Technology Development uses Project and Account Management System (PAMS). PAMS was created in the late 1990s for project management purposes, and in 2003 a requisition tracking function was added.

The multi-system approach the FBI uses for tracking requisitions may be reliable within a division, but we believe the coordination and sharing of cost data for CPIC reporting is weak across FBI divisions.

We discussed with FBI officials the future of BEARS and PAMS considering the planned replacement of FMS with the DOJ-wide Unified Financial Management System (UFMS). Officials told us they anticipate the UFMS will incorporate the requisition tracking functions of BEARS and PAMS, so that supplement systems to the core financial system will not be necessary in the future.

Funding More Easily Tracked Than Expenditures

Our testing of total costs reported by IT systems at the FBI, DEA, and JMD demonstrates that these costs can be more easily tracked when the funding for projects is earmarked in appropriations or segregated within a component's budget. However, this testing also showed that components often support IT systems from multiple sources of funding even when designated funding exists. Therefore it is difficult to ensure the costs reported for any IT system are complete.

Using UFMS for CPIC Cost Reporting Function

Weaknesses associated with DOJ's various core financial systems have been a longstanding concern. To address this issue, DOJ will be replacing the existing financial systems with the UFMS. The UFMS is designed to improve financial management and procurement operations across DOJ. It will also likely replace the requisition tracking databases at the FBI. Although CPIC cost reporting is not a requirement of a federal financial system, we believe DOJ should examine the possibility of using the UFMS to permit CIOs and other oversight bodies to obtain reliable cost data on IT systems.

APPENDIX VII

ACRONYMS

ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BEARS	Budgetary and Evaluation and Reporting System
BOP	Bureau of Prisons
CIO	Chief Information Officer
CJIS	Criminal Justice Information Services
CPIC	Capital Planning and Investment Control
CODIS	Combined DNA Index System
DEA	Drug Enforcement Administration
DIRB	Department Investment Review Board
DME	Development, Modernization, and Enhancement
DOJ	Department of Justice
eCPIC	electronic Capital Planning and Investment Control
EOIR	Executive Office of Immigration and Review
FBI	Federal Bureau of Investigation
FFS	Federal Financial System
FMIS	Financial Management Information System
FMS	Financial Management System (FBI)
FTE	Full-time equivalent
FY	Fiscal Year
GAO	Government Accountability Office
JCON	Justice Consolidated Network
JIST	Justice Sharing Information Technology
JMD	Justice Management Division
IAFIS	Integrated Automated Fingerprint Identification System
IT	Information Technology
ITIM	Information Technology Investment Manual
IWN	Integrated Wireless Network
LEO	Law Enforcement Online
LSU	Louisiana State University
NCIC	National Crime Information Center
NGI	Next Generation Integrated Automated Fingerprint Identification System
NSB	National Security Branch
OCDETF	Organized Crime and Drug Enforcement Task Force
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OJP	Office of Justice Programs
OMB	Office of Management and Budget
OTD	Operational Technology Division

PAMS	Project and Account Management System
PMO	Project Management Office
STB	Science and Technology Branch
UFMS	Unified Financial Management System
USC	United States Code

APPENDIX VIII

THE JMD RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

June 4, 2007 *Washington, D.C. 20530*

MEMORANDUM FOR GLENN A. FINE
INSPECTOR GENERAL

FROM: Lee J. Lofthus
Assistant Attorney General
for Administration

SUBJECT: Response to Draft Audit Report for Identification and Review of the Department's Major Information Technology Systems Inventory

We received your recent memorandum and have reviewed the draft audit report prepared by the Office of the Inspector General (OIG) audit staff. We appreciate the opportunity to review the draft report and provide additional insight into both the findings and recommendations.

The basis for the audit report was a congressional directive to provide an inventory of major Department of Justice (DOJ) information technology (IT) systems. The OIG provides information on DOJ's IT inventory and cost data for each of the Department's major systems, including selected cost information on three IT systems from the components responsible for the majority of DOJ's IT spending: the Federal Bureau of Investigation (FBI); the Drug Enforcement Administration (DEA); and the Justice Management Division (JMD).

We believe that the draft report's characterization that there is an "absence" of controls over IT cost reporting overstates the report's findings. We do, however, acknowledge that controls over reporting IT project costs can be improved and strengthened. While the Department does not use full cost accounting or activity based costing, the Office of the Chief Information Officer (OCIO) provides sound project management oversight on the myriad activities associated with the major technology systems inventory. Short of full cost accounting on every project, we concur that additional clarification and standardization of Department cost reporting practices would strengthen reporting reliability.

One factor that may affect the reporting of cost data but was not discussed in the OIG report is the difference between funding that is authorized, obligated, and expended. "Cost" reports or survey responses based on these different categories would likely show great discrepancies when compared to one another; however, each could be accurate.

The draft report explains the OIG surveyed components to obtain a current snapshot of project cost data as the Department does not have full cost accounting systems. We note that a survey-based cost recap performed 10 years into a project, as was the case with the FBI Law Enforcement Online (LEO) effort, does not necessarily mean that CIO or FBI did not have reasonable cost data over the decision making life of the project, nor does it mean decisions were made on materially flawed cost information. We have a similar observation about the report's findings on the DEA Concorde project. (We also note that DEA advises the draft report may contain a misunderstanding regarding its internal-use software accounting process, another factor that could have caused some of the variance cited in the draft report.)

We also want to provide additional clarifying information regarding the findings associated with the JCON project. The auditors included costs from 2000 and 2001, while the JCON project management office (PMO) did not include costs from those years in its estimate. This fundamental difference in project scope accounts for the single largest variance cited in the draft report. We believe this significantly skews the findings in the report. The JCON PMO accounts for each JCON deployment separately and as such, severs the costs as one upgrade is completed and another begins. Thus the overall costs were different because of a difference in definition, not a flaw in JCON cost reporting. We believe that this is a valid explanation for the $53M reported difference that should be recognized in the report.

Finally, the report concludes, "In our opinion, the lack of verifiable cost data for DOJ's IT system compromises the effectiveness of DOJ's IT oversight entities…" From this statement, one could conclude that no verifiable cost data exist, a finding we do not believe is supported. A more accurate statement might be that the lack of ready available "complete" cost data, e.g. direct and indirect cost data, may hamper the effectiveness of DOJ's IT oversight of some systems.

The Department is committed to reliable and effective IT project management. While a substantial portion of the draft report focuses on cost reporting, cost is only one aspect of an array of project management, life cycle reporting, earned value, and inventory management responsibilities performed by the CIO. All these activities support the management of the overall DOJ IT portfolio.

As for the recommendations in the report, we agree with the need to strengthen certain areas relating to financial reporting at the project level, and we will be studying the issue and implementing measures to bring consistency to the cost reporting.

Recommendation 1 - Ensure that component CIOs develop and implement cost effective means to report accurate, complete, and verifiable costs for individual IT systems.
Concur. The JMD Finance Staff will work with OCIO staff to look at cost accounting policies and procedures that could be improved to ensure project teams at the component level report on-going costs more accurately. CIO and Finance will also look at ways to clarify the start and end dates of projects, as timing issues may have led to the confusion on the JCON costs, and also ensure that reporting terms are clearly defined and consistent across reports and across components.

Recommendation 2 - Ensure that DOJ's CIO improves the integration of the Exhibit 53 and budget submissions in accordance with OMB Circular A-11 so that Exhibit 53 amounts can be traced to the components' overall budgets and financial systems.
Concur. We believe the Department is already compliant with the current OMB Circular A-11 requiring traceability to overall budgets. During the FY 2008 budget formulation cycle, the OCIO worked jointly with the Budget Staff to develop and implement a budget process that links the IT investment requests to the budget decision units. This data is reviewed by the Policy and Planning Staff for OCIO as well as the Budget Staff to ensure that there is consistency between the budget submission and the Exhibit 53 submission to OMB. We will verify the process during the FY 2009 budget cycle.

Recommendation 3 - Assess the feasibility of using the DOJ's planned Unified Financial Management System (UFMS) for Capital Planning and Investment Control cost reporting.

Concur. The Department will assess the feasibility of using UFMS for such reporting. However, in general, core financial systems typically track direct project costs, not indirect costs such as salaries, shared space, and other overhead costs that require sophisticated cost allocation methodologies. DOJ's UFMS is not attempting, in its initial iteration, to fulfill the function of a full cost accounting system. However, we do intend to use UFMS to track discreet project costs to the extent practicable. In addition, we agree to consider the option of a more robust project tracking capability as a future enhancement to UFMS, using the change control process which evaluates the costs, benefits and risks.

If you have any questions or concerns, please contact me on (202) 514-3101.

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT

The OIG provided a draft of this audit report to the Department on April 24, 2007, for review and comment. The Department's June 4, 2007, response is included as Appendix VIII of this final report. The Department concurred with the three recommendations in the audit report and also provided comments regarding several general issues covered in the report. In response, we made changes to the report where appropriate. Our analysis of the Department's response follows.

General Comments

In its response, the Department expressed concern over a statement in the executive summary of the report that described "the absence of control procedures" related to the CPIC cost reporting function. To clarify our intent, we have revised the sentence to read as follows: "We concluded that component CIOs lack the control procedures necessary to ensure accuracy and completeness in the CPIC cost reporting function and this likely contributed to incomplete costs reported for the DOJ IT systems we tested."

The Department's response stated that we did not discuss in our report the difference between funding that is authorized, obligated, and expended. The Department concluded that responses to our survey instrument from the different IT system project managers would likely show great discrepancies when compared to one another, yet each could be accurate. We considered that costs may be reported in various stages in the budget cycle during our fieldwork and do not believe this had any significant impact on our conclusions. Although we did not highlight in a separate section of this report how costs may be reported at different stages in the budget cycle, we described how some JCON system costs were incorrectly reported in the OMB Exhibit 300 because the program office reported appropriated amounts rather than outlays. Although the appropriated amount was accurate, the cost reporting was not correct because the cost basis requested was outlays.

The Department's response also included a statement that its lack of a full cost accounting system to identify the costs of IT systems does not necessarily mean that it did not have reasonable cost data

over the decision-making life of the project, nor does it mean decisions were made on materially flawed cost information. The objective of our work was not to determine whether the Department relied on faulty cost information to make decisions regarding IT systems, and we therefore did not make any assertions to that effect. However, from our work we concluded that cost information on Department IT systems contained in important documents provided to the Department's oversight entities was not always complete and that the Department lacks all of the necessary controls that would ensure completeness of cost reporting.

The Department's response also discussed our decision to include JCON system costs prior to FY 2002. The Department's position is that each JCON deployment constituted a separate reporting entity and that its explanation for the difference in the costs reported should be recognized in the report. Our report disclosed that the JCON PMO only provided us with cost information related to the current standard architecture, or JCON IIA. However, as stated in the report, in our view the true cost of the JCON system should include all costs incurred since JCON's inception in 1996 — which the Department did not provide — and not just the cost of the current version of the system. Therefore, we believe that our description of the costs related to JCON is accurate.

The Department's response also requested that we clarify a statement made in the conclusion section of the report concerning the lack of verifiable cost data, and we have done so. Taken out of context without the preceding sentence, we agree it may have been possible for one to conclude that no cost data was verifiable. This was not the case since much of the report details how we were able to verify some costs of the three systems we tested.

The Department concluded its response by saying that it is committed to reliable and effective IT project management. It commented that a significant portion of our report focuses on cost reporting, but cost is only one aspect of an array of project management activities performed by the CIO. We agree that the CIO engages in a wide variety of project management activities.

Status of Recommendations

1. **Resolved.** This recommendation is resolved based on the Department's reporting that it will work with OCIO staff to look at cost accounting policies and procedures that could be improved to ensure project teams at the component level report costs more accurately. The Department also said that its Finance Staff and the OCIO will look at ways to clarify project start and end dates, timing issues, and ensure that reporting terms are clearly defined and consistent across reports and components. The recommendation can be closed when we receive documentation outlining the policies and procedures used to improve cost reporting for IT systems.

2. **Resolved.** This recommendation is resolved based on the Department's response, which states that the Exhibit 53 and budget submission were integrated for the FY 2008 budget formulation cycle. This recommendation can be closed when we review documentation that demonstrates amounts reported in the FY 2008 Exhibit 53 can be traced to the components' overall budgets and financial systems.

3. **Resolved.** This recommendation is resolved based on the Department's agreement to assess the feasibility of using the Unified Financial Management System for capital planning and investment cost reporting. This recommendation can be closed when we receive documentation of the assessment.